明治大学大学院理工学研究科

2014 年度

博士学位請求論文

機械安全における停止概念に関する研究

A Study on the Stop Concept in Machinery Safety

学位請求者　新領域創造専攻(安全学系)

田中　慎也

目次

第１章　序論 1

１－１　はじめに 1
１－２　本研究の目的 3
１－３　本論文の構成 10

第２章　国際安全規格における一考察 12

２－１　国際整合規格について 12
２－１－１　標準化とその意識 12
２－１－２　マネジメント 13
２－１－３　技術影響のモニタリング 14
２－２　機械の安全方策 16
２－３　リスク 20
２－３－１　人間作業 20
２－３－２　リスク評価 23
２－３－３　リスクコミュニケーション 25
２－４　小括 27

第３章　不安の概念と停止 30

３－１　事故を防ぐ操作としての安全 30
３－２　リスク低減と安全の条件 30
３－３　不安の構造 32
３－４　リスク受容と不安の本質 33
３－５　不安のカテゴリーの生成過程 35
３－６　不安のカテゴリー 36
３－７　制御による安全 37
３－８　小括 38

第４章　防御構造の構築 40

４－１　基本コンセプト 40
４－２　安全確保のための防御 42
４－３　危険空間と安全の条件 43
４－４　危険状態の発生に対する防御 45
４－５　防御能力における制御 45

４－５－１　防御と本質安全制御 45
４－５－２　防御とその限界 46
４－６　インターロック 47
４－６－１　インターロックシステム 47
４－６－２　空間・時間のインターロック 48
４－６－３　相互・自己インターロック 49
４－６－４　安全における寿命 49
４－７　防御の階層 50
４－８　安全コンセプト 51
４－９　小括 51
第５章　制御としての安全 53
５－１　主体としての安全 53
５－１－１　主体・客体 53
５－１－２　信頼像と現実的評価（信頼性） 54
５－１－３　制御に基づく安全の要求 55
５－２　安全確認の構造 56
５－２－１　安全確認の原理の論理的関係 56
５－２－２　調整概念 59
５－２－３　人間の安全確認と調整作業 60
５－３　制御概念 63
５－３－１　調整制御の概念 63
５－３－２　安全制御システム 64
５－３－３　安全制御システムの構成 65
５－３－４　３つの制御の連係 66
５－４　安全監視システム 67
５－５　安全システムにおける停止 68
５－５－１　安全システムにおける停止と運転 68
５－５－２　停止の共通性 69
５－５－３　運転停止のリスクと階層 70
５－６　企業体と安全における認証 71
５－６－１　企業体（組織体）維持としての安全 71
５－６－２　事故を防ぐ制御 72
５－６－３　安全における要件及び停止構造 73
５－６－４　停止構造に求められる確実性 74
５－７　小括 74

第６章　空気圧システムにおける安全の考察 76

６－１　空気圧駆動システム 76

６－１－１　圧力システムにおける安全コンセプト 76

６－１－２　空気圧駆動システムの概要 76

６－１－３　本章の構成 77

６－２　安全コンセプト 78

６－３　インタロックシステム 81

６－４　インタロックシステムにおける動力源遮断 81

６－５　安全確認の条件 82

６－６　圧力監視の構成 84

６－７　動力源遮断の構造 85

６－８　故障監視における窓監視の適用 87

６－８－１　センサの故障と安全確認形センサ 87

６－８－２　窓特性の適用 87

６－８－３　ウィンドゥ・コンパレータと窓特性 88

６－９　インタロックシステムの機能 90

６－９－１　安全機能の構成 90

６－９－２　窓監視機能 91

６－９－３　停止機能 91

６－９－４　調整機能 91

６－１０　国際規格による評価 92

６－１０－１　関連する国際規格 92

６－１０－２　ISO12100-1，2 による評価 92

６－１０－３　ISO13849-1 による評価 93

６－１１　停止コンセプト 95

６－１２　小括 96

第７章　総括 97

７－１　システムにおける停止構造の考察 97

７－２　結論 104

謝辞 106

参考文献 107

第１章　序論

１－１　はじめに

近年，日本においても，機械安全のみならず安全の国際規格化が叫ばれ，主に制度面においてのグローバル・スタンダードを取入れた規格改正が急速に進められている．WTO／TBT 協定（貿易の技術的障害に関する協定）は，国内規格の国際規格との整合化を促し，また国別の認証制度が貿易障害とならないことを求めている．例えば JIS（日本工業規格）への ISO 規格の取り込みなどその分かり易い例であろう．これまでは輸出入におけるインターナショナルな境界問題と見て解決可能であったが，ボーダレスに展開される流通の健全化のために，グローバル・ルールを自国の法体系に取り込むことが求められ，それができない状況では技術・貿易立国としての日本の危機であると，「グローバル化の波が…押し寄せてきている（安全技術応用研究会，2000)」，「我が国と欧米諸国の間には大きな隔たりがある（日本機械学会編，2011)」等々，多くの警告がなされている．

しかし国際的整合化においても，私たちの国はグローバルな認証制度の考え方に適応するのが難しいとする多くの指摘（例えば参考文献（長岡技術科学大学編，2005）など）がある．現実にも，私たちの国では，認証取得がグローバルな流通条件であることの理解は進んできているが，行為（決断）責任としての自己宣言制度という観念が十分に理解されていない．依然として，事故は起こってから，その責任の重大さを問うという事後処理的体質が，今も見直されないままにあるのである．結果論として事故に責任が問われるのはやむを得ない．また，故意なら責めを受けて当然であるが，過失においてその落ち度はなかったことを実行前に示したならば（自己宣言，認証）免責の可能性を正当な権利（制度）と認めていこうという国際的整合化の本来の流れが私たちの国では形成されていない．

近年，リスクを基調とする安全の考え方が浸透してくる中，危険（源）を不可避と認めて，事故を受け入れていこうという動きが見られる．どのような条件で事故を受け容れるかが課題であるが，私たちの国では，その条件を明確にするというよりも，許容リスクは使用者によって許容されると見なし，事後の責任の簡略化（寛刑化）を求める規制緩和に利用されている．もともと規制は“最低限”として扱われ，当然安全確保の条件を満たさない．そのため，事故（結果）に対する責任も曖昧であり，規制緩和による結果責任の軽減（罪刑法定主義による追求根拠の緩和・削減）で，却って事故が増加するとしたら由々しき問題である．

国際安全規格の根幹をなすニューアプローチはローベンス報告を起源とすると一般に説明される．現実にも，先進国に限らず途上国においても労働安全等の安全規制に国際規格を取り込むにあたりローベンス報告からの強い影響を受け，認証に関わる制度の検討がなされている(大山，炭谷他，2000)．被害者を守る個別的規制からニューアプローチへのパラ

ダイム転換は国家による法規制から自主対応型，いわゆる“自主規制”への転換だとする正しい理解が必要である．しかし私たちの国では，行政による規制緩和は，個人としての主体的規制の強化であるという認識がないまま安易に規制緩和を進行させようとしていると思われてならない．規制とは本来反社会的行為の取り締まりであり，「自律できる個人」の認識がないままでの緩和は，反社会的行為の容認とも受け取られかねない．そして認証が自主規制の正当性の確認だとする理解がなされないままでの規制緩和は，却って，事後においてどのように責めを受けるか分からないという社会的不安を生む．

事故の回避の追求の結果としてやむを得ず生じた事故に対して，賠償（金銭）によって事故前への復帰が約束できれば，社会は事前の安全配慮の限界を認めるというのがグローバルな安全だと言っていい．私たちの国の民法（不法行為法における賠償）も同様の考え方である．改めて，安全において，事故を受け容れるための社会的合意があり，それに正しく準拠したことの実前の確認が“認証”であるが，日本では制度としての認証が曖昧であるために，結局，事前のチェックが十分になされないまま事故を起こし，必然的に不備を指摘されて安全配慮義務違反や業務上過失責任，あるいは善管注意義務違反等の追及を受ける．また PL（製造物責任）法においても，消費者保護・救済のため，製品による損害が生じた場合，企業（製造者）に立証責任を求めるが，事故は欠陥の存在の明確な証拠と見なされ，私たちの国では，事故の原因に対する予定責任（認証）よりも，結果責任として事故の追及がなされる．いずれにせよ，私たちの国では，安全は事故の予防であるにも拘らず旧態然として安全性の向上が事故の経験（結果の追求）を必然とするという矛盾した法体系の下にあって，近年の国際規格の国内規制への整合化は，これを根本的に見直すべき要請だと考えられて当然である．

本来安全には，少なくとも重大な被害を伴う以上，「経験することも経験させることも許されない」とする条件で予測回避すべき要求がなされる．そのような深刻な被害を与えるのが事故である（そうでなければ，事故の被害は損／得の単なる“損”でしかない）．しかし安全が，事故（結果）の予測（リスク）という認識で，結果でしか評価されない現状にある私たちの国では，事前に講ずべき技術的方策に正当性（認証を事後の免責とするような）を求めるという視点に立てない．それゆえ安全の“水準”とは，今も結果の評価（確率論）で表すという制約から抜け出せないでいる．

滅多に起こらないのは当然だが，その中にあって特に予測回避が強制（証明の要求）されるような事故こそ安全の対象であるはずである．自己宣言のためには理論的根拠が不可欠だが，実行前の立証責任が曖昧な私たちの国では，安全の理論体系の構築（安全を保証する安全工学の構築）が進まないでいる．

科学は実験科学と言われるように実験により理論の検証を行っている．しかし安全とは人間への直接的被害に関わるから，人間に試してみてその死傷率で測るようなものではない．医療でも食品でも，市場に出す前に何段階も確認があり，また市場に出ても安全が確認できないときは回収しているはずである．単に確率の問題ではなく，“確認できないとき

は安全側（使用停止，回収）に”という判断が連鎖しているはずである．そこには，渡されていく過程で，ある程度の危険を覚悟で受け入れていくことになるかもしれないが，残る危険があるからこそ確認のための理論が求められる．求められるのは安全を確認するための理論とそれを実施するための制度である．

１－２　本研究の目的

“安全の原理”（杉本，蓬原，1990）は「危険を伴う行為は安全を確認して実行され，安全が確認できなければ実行されない.」と明快である．これまで多くの研究から安全確認システムの有効性が示され，また国際安全規格は基本的に安全の原理に矛盾するものではないと説明される（例えば（梅崎他，2001））．しかし国際安全規格でリスク概念が提示され，あくまでも安全はリスクで扱うことであり，リスク論こそが安全理論であると私たちの国では考えられている．安全確認システムにおいても，「確認」も「停止」も失敗を確率的に認めるとする前提に立ってリスクで扱うことがグローバルに整合的だと解釈される傾向がある．

リスク論は大きな事故も小さな事故も確率（頻度）を考慮してリスクとして評価し，同じリスクなら，同じ被害として扱おうとしている．しかし事故の経験を繰り返し可能（頻度としての扱いが可能）とするのは機械の提供者（加害者）の立場であって，被害者がそれを経験するとしても一度であり，しかも金銭的賠償で原状に復し得るとしたら，明らかに小さな被害でしかない．私たちの国でも，リスク（損害の期待値）を用いて，損害を予め許容レベルに抑えるという“予防”の考え方が取り入れられつつある．許容リスクは，事故（結果）に対する免責を意味していない．それにも拘らず，リスクに対する勝手な解釈で，もともと金銭による賠償を計画できるはずがない死亡事故や，一旦起こったらどんなことをしても償えないような大きな被害の場合にも，リスク（被害の可能性）が小さい（結局のところ確率が小さい）として予防を軽視したり不要と決め込むような自分勝手なリスク解釈が生じうる．許容リスクという概念を導入して，事前に安全問題が解決されたと思い込むことで，逆に安全を曖昧にし，社会的混乱を生じかねない状況にあると言える．

事故には，「取り返しがつかない」と見なされるような致命的と言える被害が存在する．結果論として扱い得ない対象であるはずだが，一度も起こってならないとされるべき致命的被害の事故もリスクで「許容」を判断するように適用が拡大されていると思えてならない．起こしたら，何らかの事後処理（例えば保険）を取られざるを得ない．それは死亡事故でも金銭賠償で済ますことになれば，逆にその実績が感覚を麻痺させ，死亡事故は金銭で「取り返しがつく」ものとして扱われるようになってしまう．

取り返しがつくからこそリスクで扱うこと（繰り返せる）ができる．本質安全（危険源自体が存在しないまたは影響が問題にされない状態）で起こるトラブルなら，特に“リスク”を持ち出す必要を生じない．しかし，許容リスクとは言え，容易には受け容れがたい

重大な被害を伴うものであれば，（繰り返しは許されない条件で）1 回の経験だけが「取り返しがつく」というリスクで扱える限界であると言っていい．リスクベースの安全は，予測される事故の被害が経済的損失と割り切って金銭的賠償が可能だという場合に限定されるということである．被害の期待値としてのリスクは加害者が請け負う金銭的賠償であり，賠償の対象は例えば被害者の損失日数に係わる．事故の被害で“お金”が直接動くわけではないかもしれないが，あくまでもリスクを事故（結果）の責任に対する予測（被害補償の期待値）とし，小さなリスク対して許容の判断を行うには，お金の有する合理性（客観性）に依存せざるを得ず，リスクに経済的合理性を適用することで，安全は，経済的損失に対する補償の制度として実現されるのである．

さて，被害者が被る取り返しがつかないと言える事故は，同様に加害者にとっても取り返しがつかないと考えなければならない．すでに述べたように，リスクが許容レベルにあるか否かに関わらず，被害に対する金銭的賠償が適用できない“取り返しのつかない事故”は，あくまでも事故の前に「停止」を確保して“確実に”事故を防ぐとする方法論が確立されなければならないはずである．

本論においては，「取り返しのつかない事故」とは，どのような代替（賠償）によっても原状に復することが不可能であり，事故の前に「止める」ことに曖昧さを許さないような事故だと定義する．「止められるのに止めなかった」とする後悔（結果論）を認めないという安全が構築されなければならない．本論では，事故を防ぐとする安全本来の目的とリスクベースとする国際的な安全の方法論との関係性について検討される．

ところで，欧州認証制度（例えば CE マーキング）は，欧州規格に準拠して，実用の段階に入る前（事故となる前）に講じた安全対策によって，低減されたリスク（事後の責任）を確保しようとするものである．事後の責任（リスク）の軽減を期待するためには自分勝手なやり方は許されない．制度として，何よりも“安全”に対する整合性が求められる．事故は安全対策の失敗（欠陥）で起こり，「安全対策の失敗」は，事故の前に停止できないことであり，このような故障は「危険側故障」と言われる．事故は危険側故障によって，事故の前に停止できないために発生するという共通の認識が成立することになる．これにより，安全対策の欠陥で事故の前に停止できないために生じた被害の期待値をリスクとするという安全の整合性が得られ，リスク低減のための安全規格が整備される．さらに，安全規格に準拠したことの確認を認証として流通の健全性を確保するのが安全認証制度だと理解される．

本論で特に強調したいのは，“事故を防ぐ”とは「事故の前で止まること」として，これを，安全を論ずる場合の共通認識（原点）としていることである．事故は，事故防止の欠陥で生ずるが，事故の前に止まることの失敗であり，停止完了が「遅れること」で危険状態となり，結果として事故へと繋がるという認識を共有する．さらに，停止の失敗で生ずる被害の期待値をリスクとすることで，リスクとリスクベースの安全の関係性が示される．特に，「取り返しのつかない」で象徴されるような致命的被害が予測される状況では，リス

クベースの安全は適用できない．その場合は，事後の責任の予測（リスク）を論ずる代わりに，事故の前で確保されるべき「停止」のために，停止が“構造”の条件で実現されなければならない．

さて，ここで，リスクベースとする国際安全規格と安全の原理との関係性に触れておく．“事故を防ぐ”とは事故の前に停止することだと述べたが，そのためには，安全の原理の示すところであるが，安全と言える制限を超えるとき，危険を知らせる（停止を要請する）ところの安全確認システムが構成される．国際規格は，安全確認システムをリスクで評価するが，システムの危険側故障，すなわち「安全の制限の逸脱による停止」の失敗の可能性を持つ故障によって生ずる事故の被害の期待値をリスクで表し，広く「許容」と合意される判断基準を許容リスクレベルで示している．危険側故障（誤り）には大きくは安全の制限を逸脱するという制御（管理）の誤りと停止すべきとき生ずる停止の失敗とに分かれ，これらが重なって事故が発生するから，事故の被害の期待値は明らかに確率論的（リスク特性）であると言える．

製品の設計は個別具体的であり，その安全条件は製品によって異なるが，安全の条件を逸脱した場合停止すべきことは安全確保の共通の原理である．安全確認システムは，安全条件を規定し，危険側故障（誤り）で生ずるリスクをどのように最小とするかを指向し，さらに，取り返しのつかない事故の場合，リスクを生じない条件で，事故の前の停止を如何に確保するかが志向される．これらの追及は明確に区別されなければならない．

例えば，BS EN 764-7（火なし圧力容器の安全システム）（BS EN,2002）ではリスク低減と停止によるリスクの本質的抑制の両方が規定されている典型的な例である．本規格の序文にて，制御操作の構成図（Fig.1-1）で，“事故の前の停止”の実行部分が運用システム全体のどの部分かを示して，これを安全システムとしている．それは逆に危険を伴う運転システムの本来取るべき制御の構成を示していると言える．

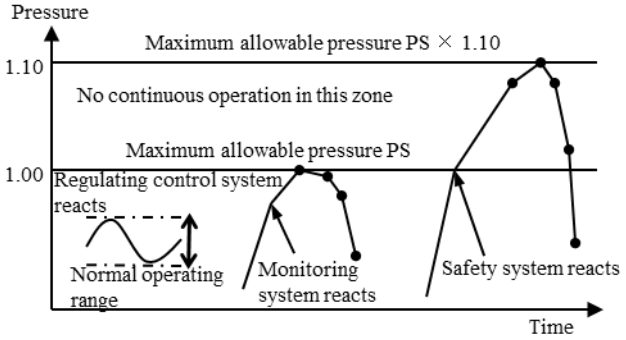


Fig.1-1　PS との関連における調整，監視及び安全システムの応答（BS EN,2002）
最大許容圧力の中において運転制御が定められ，運転範囲の逸脱を，許容圧力から逸脱しないように調整される．許容圧力の逸脱においては連続運転を許さない停止が行われる．ここでは停止において最大許容圧力の 1.1 倍を逸脱しないことが要求として定められている．この最終的な制限を安全システムと限定し，他は安全規格から除外している．

本規格は，圧力装置は設計の段階で，破裂事故が破壊圧力を超えて生ずると想定し，通常の運転（Fig.1-1 の Normal operating）で破壊圧力を超えて使用されるのを防ぐための基準に，許容使用圧力（Fig.1-1 の Maximum allowable pressure）を安全条件として規定する．そして許容使用圧力を超えないように（安全条件を逸脱しないように）管理制御（Fig.1-1 の Monitoring system）を行っている．このことは，許容使用圧力の中に在ることが安全条件であり，圧力容器はリスクを生じない条件が許容使用圧力をしきい値として判断され，それを超えない使用ではリスクを生じないことを意味する．すなわちリスクは，許容使用圧力を超えた使用の可能性（危険側誤り）で発生し，安全条件の逸脱でリスクは事故（破裂）として発現する．

このように，規格において運転システムの挙動をリスクで評価するに当たり，たとえ信頼性であっても，安全条件を維持してリスク発生を抑制する管理制御が前提にあり，誤ってこれを逸脱することでリスクが発生することを明かにしている．しかし，すでに安全システムの存在で暗示されるように，管理制御の信頼性に依存するだけでは，明らかにリスクが大きい．そこで，安全条件を維持する管理制御の制御結果を監視／確認して，安全条件を逸脱すると停止操作（Fig.1-1 の Safety system）が実行される．これによって，安全条件を維持する操作の誤りで生ずるリスクは確実に解消される．しかし，本規格における停止処理とは逸脱を回避する機能としての停止であり，本論に示すような「事故の前に停止すること」を確保する安全システムとしての構造が本規格では明確にされていない．

一般に安全規格における最大の特徴は，安全方策（安全機能）の故障の仕方を規定している点であろう．安全条件の逸脱を検知する装置は実用的には高い信頼度を要求するが，安全性の立場からは非対称故障特性（危険側故障が発生しない特性）を要求する．しかし，国際規格のこの要求は，一般には，例えば多重化や故障診断等で安全側故障に偏らせることで実現されると見られている．国際規格がリスクベースであるために，どのような基準も，リスク概念で追及可能，あるいは多様な方法を組み合わせてリスク低減が可能だと信じられているのではないか．このような信念の下では，“確認”も“停止”も，様々なリスク低減の一手段でしかなく，あくまでもリスク低減効果が大きい方が優先される．そうなれば，リスク低減には，信頼性を上げて低リスク状態の運転を確保しようとする方が，停止させてリスク発生を防止するより優先されてしまうのは当然であろう．このことが，「事故の前に停止すること」による安全確保が積極的に導入されない理由であると思われる．

しかし本論は，運転仕様ではなく事故防止に根拠を置く．事故を明確に捉え，「事故となる前に停止する」の構造を確保することが運用システムの最優先の規定であり，そこに依拠（depend）して運転仕様が適用されることになる．それに依拠する構成とは，安全条件を維持する“制御”と“停止”とが互いにリスク低減を分担するというやり方でなく，事故の前に停止する構造でリスク発生を抑止する構造を最後的手段としてまず確保した上で，できるだけ停止しないために高い信頼性に依拠する管理制御を実行するという関係となる．

残留リスクを「危険の扱いの限界」として認識するとき，事故の前に必ずしも停止でき

ない事態が起こり得ることを意味する．制限を無視して事故に接近したことで事故が起こる．危険を扱う限界は停止して事故を防ぐことで，本来残留リスクは解消されるはずである．「危険を扱う限界」とは，結局，危険なものを安全に扱うということの限界（確率論）と考えるのでなく，危険を扱えなくなったら，事故の前に扱いを止めることだということができる．そして，扱いを止めるべき限界に来たかどうかの確認が安全確認であり，“限界”の判断で扱いの停止を確実に行えばリスクは完全に解消される．人間に安全確認を委ねた場合，限界を見過ごしたり停止の決断が遅れたりで，リスクで評価する以前に事故防止が殆ど期待できないだろう．そのため，安全の条件を維持する操作を人間に委ねても，現実に安全の条件を逸脱していないことを工学手段を用いて確認して，確認できない場合は強制的に停止する方法（フェールセーフインタロック）が講じられる．人間は信頼性の低い制御装置であり，また事故の前の停止の要求に必ずしも応えられないような不安定な安全装置であると認めざるを得ないから，リスク低減を人間と工学的手段による停止で分担するというよりも，運転システムの全体として，事故の前で止まる安全システム（Fig.1-1 の Safety system）を工学的手段が担当し，安全と無関係の信頼性（確率論）に委ねられる操作（Fig,1-1 の Normal operation と Monitoring system）を人間が分担するという関係でシステムが構成されると考えていい．したがって，安全システムによる停止構造を有しない運転システム（例えば原発）では，停止による事故防止が保障できないので，少なくとも取り返しのつかない重大被害の可能性がある場合は，適正な運転システムが構成できないと認め，安全工学の立場からは運転は許可し難いと言わざるを得ない．

一般にリスクベースの運転システムでは，運転仕様を設定し，安全の条件からの逸脱をリスクとして対策を計画する．そこではあくまでも停止はリスク低減の一手段である．しかし本論においては，事故を回避するための停止構造を最優先に講じた条件で，運転仕様（安全の条件）が実行性を持つ．つまり，運転仕様（安全の条件）を逸脱することで生ずるリスクを軽減するという考え方でなく，「事故の前の停止」の条件を優先的に確保した上で，先んじて停止しない操作を行って機能上・性能上の効果を最大限獲得しようとする運転形態を構成すべきだというのが本論における主張である．多くのリスク低減要素（安全機能という）が総合して全体のリスク低減効果を上げていくとする設計ではなく，事故との関係で定まる安全の限界を明確にして，「事故の前に止まる」を「安全の条件の逸脱において止まる」として実現し，リスク発生自体を抑止すべきこと，ここに安全の基本原理を求め，リスクベースとは異なる安全な運用システムの存在が示される．

本項最後に，人間機械系における安全概念について触れておきたい．機械安全（ISO12100）におけるリスク概念は，人間の傷害にリスクの対象を限定している点を特徴とする．許容リスクレベルの適用範囲を人の傷害に限定することは現実的要請であるかもしれない．また完全な無人化で人が居ない作業場の実現には限界があり，人の傷害リスクの低減は普遍的な要請であるからだとする理解も可能である．このことは，機械安全は機械の人間との関わり方として本来あるべき要求を示すものであり，“安全な機械”ではなく“安全に機械

を使用する”を求めていると考えていい．それ故，リスクベースの安全は，機械と人の関係において，機械が人に与える危害可能性（リスク）を人が許容リスクの条件で受け入れていこうとする姿勢の表れと見ることができる．機械安全は機械と人間との共存（協働）を意図しており，本論では，この共存状態の確立において“停止”が決定的な役割をなす点に言及する．

共存とは，もともとリスクのない状態の構築であり，それが隔離原則と停止原則で説明される．しかし，人と機械の関係は，単に「離れていればいい」ではなく，互いに近づくことが求められ，メンテナンス等では人が機械の中に入る状況さえ作られる．許容リスクの条件で機械が人に与える危害の可能性（残留リスク）を人が受け容れるとしても，少なくとも耐え難い重大な被害の可能性は確実に排除されていなければならない．そのための機械の運用システムは，人に危害とはならない条件（安全の条件）に関する監視がなされ，その条件を逸脱した場合は速やかに停止が実行される．すなわち，“停止”を最後的手段として人との共存条件からの逸脱を防いでいるというのが機械の自立性に依拠する安全と共存に対する理解である．停止の遅れで致命的重大事故が発生することは許されない．これを防ぐための安全確認システムでは，安全条件の逸脱を検知して停止するという危険検出型の考え方でなく，安全の条件の確認ができない事態を生じたときは，いつでも停止状態（無条件な保証，本論では無可能状態としている）に移行して，少なくとも危険側故障（誤り）の発生を防止する．

人を受け入れるべき立場の機械は，人との共存可能な状態（安全状態）を停止から考えるべきである．「リスク低減のために停止する」ではなく「共存のために停止する」とすべきとする主張である．身近な例では，設計で，バリやエッジを気にするのは，停止状態の共存において人に危害を加えないという理由によるからである．

人との共存を安全の目的とするからこそ，機械は，人への危害可能性（リスク）に対する限界に深刻に対処する．安全規格では表面的には見えにくいが，安全の条件とは未来の事故による影響（ポテンシャル）に対する対応可能性の限界を正しく把握しているかに証明性が求められ，それ故，その限界における危害が評価され，限界を超えていないことの判断で証明性に応えるのである．私たちの国ではシステムの危険側故障を，結果としての死傷率で測り比較することが行われるとすでに述べたが，実感として昨年より死傷率が低いからと言う理由は，事故回避（予防）が正当に行われたことの証明にはならない．また現在事故が起こっていないということも安全であるという証明にはならない．事故の被害の対応が「自分には無関係」という立場で，安全との関わりからの逃避でしかない．

人との共存を確保する手段として機械システムの“停止”があると述べた．フェールセーフによる停止の確保は，停止後の修理のための人の接近を求めるための機械側の安全／共存の条件である．

人に危害を加えない確実性を確信するためのシステム（構造）が求められる．安全確認システムは，想定した安全条件を想定通りクリヤーするだけでなく，それを立証（確認）

して想定の通りの機械の運転が実行され，また，立証（確認）できないときは想定通り停止する．これにより，既知の危険においてその対処を曖昧にしないことが求められており，想定外に対して停止を想定するという関係がリスク概念を生じないとする理由である．リスクアセスメントは，事故を想定することの重要な手続きだということができる．しかし，改めて，リスクで扱える条件（起こることを許容する）に在るということは，リスクで扱えないこと（取り返しのつかない被害）は徹底的に排除したという事実に依っていることを忘れてはならない．そして「取り返しがつかない被害」の可能性を持つ危険源の扱いを要するシステムは「事故の前に停止する」ことが保証できる安全確認システムを実現しなければならない．停止できなければ，取り返しのつかない事態が待っていると考えられるからである．

機械安全におけるリスクベースの安全は機械（危険源）が人に対して生ずる事故（accident, 偶然の事故）を扱うものである．しかし，事故回避の限界としての偶然性を社会的に解決すること（結果論としての救済，保険）ではない．事故回避が偶然にできなくなる状況のためにこそ，“停止”による最後的手段が確保されていなければならないからである．本論にて示す安全の原理の例として示す空気圧システムの構築において，国際規格による評価を行い，国際規格の条文から安全の原理を見出せること，つまり国際規格の基本が安全の原理があるという見解を示し，よってこれらは矛盾するものではなくむしろ本論は国際規格（ISO12100）における一般設計原則が安全の原理の準拠し補強されるものであること示す．本論が指摘するのは，人と機械の共存において，機械の停止が遅れることで人との接触が生じ，そのためリスクが生じることを示し，その対策のために構成される安全確認システムは，危険側故障（誤り）すなわち危険なときに停止が遅れる側の故障を生じない条件で，取り返しのつかない被害の防止に適用されることを示す．

国際規格（例えばISO13849）では，安全確認システムの安全性を危険側故障の発生確率で評価しようとしている．本来，停止可能であるから危険を扱える．つまりもともと危険を生じない条件で安全を達成するのではなく，事故（危険）を見据え事故となる前に事故へのプロセスを停止するのが安全確認システムである．それ故，停止による安全確保ができないような機械があれば適用できない．停止が安全の最後的手段であることは明らかであり，これが確保されない条件で運用が許容されることがあり得るとしたら，事故に対する結果責任がどうにか取り返しがつくと言える軽微なためであろう．すなわち，確率論（危険側故障の発生確率）で安全性を評価するかぎり，国際規格は取り返しのつく軽微な被害であることに限定して，リスクベースの安全を展開していると考えていい．本論では，リスクを生じない安全確認システムを要求する点で，国際規格よりさらに限定的と言えるかもしれない．しかし，停止による安全確保を曖昧にして，停止できる機械を停止できない機械と同様にリスク概念を用いて扱うことで結果責任に混乱を生じていると言える．

機械安全における３ステップ・メソッドも，リスク低減（信頼性）の３重化ではなく，非対称性の３重化として理解できる．本質安全設計における欠陥，付加防護策（ガード等）

における欠陥，情報提供における欠陥において，安全確認システムの概念から，それぞれ欠陥は“停止”へと導かれるとされる．本質安全構築（制御）の失敗は停止へ，ガード（隔離維持制御）の失敗（故障）は停止へ，人間による安全管理（制御）の失敗は停止へと繋がるものであるが，結局これらの停止の失敗がリスクで評価され，許容の判断（結果責任が取り返しがつくか否かの判断）に委ねられることになる．このように停止の要求の不確実性を許すのは，被害が経済的損失をお金で補償するように，取り返しがつく範囲に限定しているからである．

本論における“停止”とは，リスクのない状態の人と機械との共有であり，安全とは停止に依拠する(dependable)ことの妥当性である．安全の原理（杉本，蓬原，1990）とは停止による安全の確保をユネイト（杉本，粂川他，1988）の関係で実現することであり，危険源を設計上排除するという考えでなく，“停止”によって危険との接触（事故）を防いでリスクを生じないこと（妥当性）を安全確認システムとして実現しようとするものである．

１－３　本論文の構成

安全の原理（杉本，蓬原，1990）等，過去に進められた研究と，国際的な安全の整合である国際安全規格（主に機械安全規格）が妥当な関係であることは過去にも主張されてきた（例えば（梅崎他，2001））．本論においては，その拡張的な概念（自己制御）を示すものであり，それは制御と評価の関係であり，主に評価の部分で検討されてきた過去の議論とは矛盾しないものである．またそれ故に，機能安全として拡張される安全規格に対しても妥当な論理を与えるものと考える．

第２章において，国際安全規格を俯瞰しながら予備的考察を行う．欧州の機械安全の日本での理解はリスク評価であるが，その中で“隔離の安全”“停止の安全”（向殿，2003）と分析されており，またこのことが日本における安全装置メーカー等の国際安全規格の紹介などにおいて広く利用されている．しかしその利用においては，概念というよりも具体的対処（ガード，ブレーキ）として認識されがちであり，概念としてありながらも十分に分析されてはいないと思われる．そこにはインターロック構造（確認構造）があるものと認識する必要がある．

第３章においては停止が不安（リスク）を解消するものと述べ，第４章，第５章において本論は停止を基底においた確認構造から考察しなおした制御概念としての安全を検討する．それはシステムにおいて目的機能が注目されるが，そのシステムの存続がおろそかにされており，自らの存続を確約するのが停止であり，安全は停止構造からその展開を検討することであると主張するものである．そして第６章において本論による安全システムは現行の国際安全規格と整合が取れる構成であることを論ずる．本論で示される構成は「安全の原理」（杉本，蓬原，1990）等で進められた研究を援用することで証明の補完とするものである．そこにおいては「安全の原理」により妥当性を得るものであると示す．

結論として，本論で提案する論理は，安全の原理等の確定的な安全と国際安全規格等のリスク論（確率的）の安全を矛盾するものとして扱うのではなく，統合的に理解することを主張するものであり，停止構造こそ人間と共存する機械が持つ本質的な構造であると主張する．

第２章　国際安全規格における一考察

２－１　国際整合規格について

２－１－１　標準化とその意識

元々，規格は部品を標準化することで，一品モノではなく分業・大量生産，交換・修理の容易性ということへと繋がったもので，生産・運用におけるマネジメント的意味合いも強い．自社規格で顧客の代替可能性を奪うことでの囲い込み等の時期もあったが，海外展開・国際調達という時代になると，国際的に整合のとれた規格で作られたものでないと，クリアランスの調整に膨大なコストをかけることになる．インターナショナルの時代は相手国との調整でよく，アメリカへ輸出するならアメリカ向けと調整し，東南アジアなど JIS 規格が受け入れられる時代は日本製をそのまま提供すればいいような時代であった．しかし東南アジアにおいても様々な国と輸出・輸入をし，各国が様々な形で世界中と繋がるとき，各国間の調整ではなく各国を超えた共通のものに対して各国はキャッチアップするという形が取られるようになった．それがグローバル・ルールであり，グローバル・ルールを取り込んでいくことで，各国・各企業と共通に繋がるということを可能にしようという流れである．それは WTO／TBT（世界貿易機関 World Trade Organization／貿易の技術的障害 Technical Barriers to Trade）協定により，国際規格として世界の流れは方向付けられ加速されている．

国際整合規格も EU（欧州連合）の整合化にその範があり，それゆえ EU で既に整合されているものには説得性があり，その経験もあるため EU がイニシアティブをとる形になっている現状がある．日本人的感性からすると「世界統一の純粋な心持で集まる場ではないのか」といった感覚があり，それ故，日本人から見ると EU の世界支配戦略と見えてしまう．

ルールは「与えられる」ものといった感覚が強い日本と，ルールは「自分たちで作る」という感覚が強い欧米において，日本人は欧米にルールを押し付けられるという感覚を抱く．国際的な整合の流れにおいて規格整合を作ることにおいて，押付感は緩和されるが，日本人は「ルールが与えられたのでそれを守る」という感覚であっても「作る」という感覚には乏しい．それは，日本人の法意識において法概念が十分に形成されていないせいかもしれないが，それゆえ自然法と実定法の区別があまりできないともいえる．実定法は人が作るものであり，現代では主権者である市民（を論拠として）により定立される（直接的ではないが）ものである．しかしそこでは自然法という原理的な法に背くことは許されないという観念を持つ．国際規格においてはこの自然法と実定法の関係における実定法の部分であると相似表現できる．そしてルールとして明記されない観念が形成されているこ

とに注意をする必要がある．ルールを守ればいいではなく，良き実践の中に良きルールが形成されていく．これまでの歴史において，日本では市民革命といった啓蒙を経ず，国家や大企業の絶対的な立場からのルール提示という状態に適応してきたため“作る”という観念に乏しいと考えられる．それゆえルール逸脱（違反ではなく不明瞭な点に関して）に対しても抵抗があり，欧米では逸脱はリスクアセスメントで対応，できないルールは（原理に戻って）修正すればいいとなるが，日本では与えられるルールに対して絶対的感覚があり逸脱も修正もできない．また逸脱において，欧米では個人（企業）の責任において判断を行うが，日本では個人の責任であるが故にそれはできなくなってしまう．それゆえ役所に判断を仰ぐといった行動になり，また当然その判断について自らの正当性を裁判で争うということもない．そもそも，国際規格は法律違反を促すものでもなく，法を優先するように求めるものであり，それゆえに法システムの国際的整合が要請されるものである．

２－１－２　マネジメント

一時期，技術経営が持て囃されていたが，マネジメントしていくにはまず技術が評価可能かというところがある．価値を認識しないところに行動はなく，価値はどのような概念を持っているかで変わってくる．マネジメントが単に金銭評価であれば，世の中にあるものでしか評価できず，これから世に出すものは金銭評価に載らないので，二番手戦略，類似戦略的になりがちである．またマネジメントが技術者的評価であれば，技術の追求になり商品開発とはかけ離れてしまうことになりがちである．マネジメントが市場に価値ある商品を提供していくにあたって，技術に対しどのような概念を持ち評価・コントロールしていくかという問題になる．

国際的な規格の整合化は進んでいるが，大きく変化したのが ISO9000（品質マネジメント）あたりからで，部品ではなくマネジメントに注目が集まった．これは企業間の取引において単純に部品の外形的整合等が取れればいいだけでなく，様々なこと（品質）を統合的に扱う必要へと進んできたためであるが，そのような品質に対してマネジメントとしてどのような概念を持って評価・コントロールするかという問題となってきた．ISO14000（環境マネジメント）も ISO26000（社会的責任）や OHSAS18001（労働安全衛生マネジメント）も同様で，マネジメントとしての概念形成のための共通指針である．

国際安全規格は一般には強制ではなくアドバイスであるとされる．それは個々の製品により安全の仕様は異なってくるゆえに強制ではない．また国家は労働安全などその扱いが人権にかかわってくるからこそ，不当な人権侵害を除去する目的で強制を行うことができる．そして国家による予防的強制を回避するためにこそ自主管理の正当性を主張する．

労働安全衛生マネジメントシステムは，法規制に対し自主管理の正当性を示すことで，法体系自体が細部まで条文で言及し企業の身動きが取れなくなるような複雑さとなること

を回避する，という関係性が期待されている．機械安全（国際安全規格）も労働現場への機械の導入という点で，その法体系の中に在るものであり，自由な流通のためにこそ，その法体系の下で自らの正当性を示さなければならない．マネジメントは自らの選択可能性を確保するためにこそ，自主管理の正当性確保が重要となる．

国際規格の使用は，正当なアドバイスを参照することで，自身の正当性を示すことが目的である．この点はマネジメント規格において特にそうである．マネジメント規格が正当であるからこそ，それを論拠にすることに正当性がある．日本の品質は世界一だと豪語しても，自身の正当性は示せない．認証においても，品質の国際規格という共通性があるからこそ，そこを基準に認証できることになる．日本企業は，自分たちの品質は良いので，国際規格に依らないで自分たちのやり方を認証するように要求すると言われる．「自分たちは良い」を認証するのはその基準点が特殊的であるがゆえに難しい行為になる．

そもそも自身の正当性を示したいという欲求があるのか，その場合，同様の欲求を持つ他者に対してどのような相互性が要求されるかという問題がある．他者に正当であることを求めるからこそ，自身も同様に正当でなければならない．他の方法もあるだろうが，一つの方法として，規格が正当であり，かつ，認証が正当であるから，ゆえに，自分たちは正当である，と言える．しかし，自分たちの正当性を示したいという要求がないところでは，規格が正当であってほしいという要求もなく，認証会社に対し認証に嘘は入ってほしくないという要求もない．また，他の企業に“認証会社”に疑義がつくような行為は行ってほしくないという要求もない．自らの正当性を確信したいからこそ，自己確認の正当性をどう担保するかが重要になり，社会制度としての確かさとしての形成が要求される．

現状日本では事後の制裁としての行政システムに多大な幻想を置いていると言える．行政が純粋に被害者の味方になってくれるという安易な幻想とそれによる予防効果である．それゆえに事前の信頼形成は必要とされないと考えられる．

２－１－３　技術影響のモニタリング

国際安全規格（機械類の安全等）は一般的なマネジメント規格ではない．技術者における，安全に対する概念の共通化であるが，企業という組織体において，その安全を要請するのはマネジメントであるという視点での共通化と考えることができる．また，機能安全は品質同様捉えどころがないものをコントロール（維持）して行こうとするゆえにマネジメント規格的な体裁になっていると考えられる．国際安全規格では“絶対安全はない”を前提にしている．しかしそれは，リスクが小さければ被害の影響を無視していいと述べているとは考えられない．むしろそれゆえに被害の影響を小さく抑えるのみならず，その被害としての結果に対して責任を持つことを求めていると考えられる．それが合理的な補償としての保険システムになっていると考えられる．そもそも，リスクを扱うとは，何ら

かの形で「取り返しがつく」からこそ可能と言える．それを引き受けられるが故と言えるが，一般化されたのが金銭賠償であろう．それであれば本来，金銭賠償とすることが社会的にも可能な範囲でこそ許可されるはずである．リスクとは衡平性が担保された契約において，価格が形成されることとなる．マネジメントシステムは，よく PDCA（Plan・Do・Check・Act）を回すと表現するが，妥当な基軸に対して回っている状態が自身の正常性であり，単に環境に反射するのではなく，自ら環境に作用してそれへ対応能力を確認するからこそ，真に環境変化に対応する能力があることを確認することができる．ここにおいて，安全マネジメントシステムを回すとは，どういうことになるのであろうか．

マネジメントは製品を世に出すとき，それは技術の持つ社会的に負の影響に責任を持つことであり，それ故にその影響をコントロールしなければいけない．「良い商品は良い」ではないし「悪い結果が起きなければ良い商品」でもない．もし，良い商品を出すのならば，その良い商品をどう守っていくか，それ故にリスクを検討しその発現を抑えるべくマネジメントとしての役割がある．

その商品が社会的に求められているから出すのであれば，その良い商品を社会から失わせないのがマネジメントの役割である．人を助けるための製品など，良いものはたとえ事故があってもユーザーがその存続を望むかもしれない．しかしメーカーとしてリスク・ベネフィットで「良い製品なのだから被害は社会・ユーザーで受け入れて当然」では，そのメーカーは社会的存立を危うくする．

技術者・設計者は自分なりに安全な製品を作っているかもしれない．しかし作って終わりではない．社会に出てから，予想のつかない様々な使われ方が行われるかもしれない．大人が使うことを前提としたものが子供の手に渡るかもしれない．その影響が社会的に十分に許容内にあるものであればともかく，リスクが高い製品は「十分に想定したから大丈夫」ではなく，想定内であり大丈夫であることを社会においてモニタリングする必要がある．モニタリングするからこそコントロールのための情報を得ることができる．そのためにはマネジメントとしての実行が不可欠である．

例えば，モニタリングするということは想定内であることを確認し想定通り対処することであり，昨今ではソフトウェアのアップデートによる問題点改修がわかりやすい例である．そしてリコールはマネジメントによる製品の停止行為であり，想定内と確認できないとき，社会的に対処できないほど影響が拡大する前に停止（大規模・明示的な回収や補修・交換）することである．そしてモニタリングは，マネジメントが技術の影響プロセスを理解できなければ行えず，モニタリングにより状況を認識できなければ影響に対しコントロールできない．

ISO12100（機械類の安全性）は技術者のための規格であるが，そこに通底するリスク概念はマネジメントに理解可能な情報を提供するための指針と考えるべきである．またモニタリングは単に製品メーカーだけでなく，製品を使用する企業においても同様である．ユ

ーザー企業においても信頼性 100%という在りえないことを求めるのは，自分たちの仕事を不確実性にさらし，自らの仕事に対して不誠実である．当然，メーカーの意図に対し，正しく使い，また，その逸脱による負の影響も考慮しながらその発現を抑えるように扱う．そしてそれは，正しく使われていることを確認（モニタリング）することによって担保される．そして確認できなければ“使用をやめる”ことによりリスクが発現しない基本作業であることが示せる．このコントロールを行うという概念があるかどうかで対処が大きく異なる．コントロールを行う企業はメーカーに危険源とその影響プロセスを求める．つまり危険が，可観測であり可制御であることを求め，これは“安全に扱う”ためである．そして“安全に”という概念から外れる前に“やめる”ことで安全を確保することができる．

しかし当然ながら，“大きな被害”を起こしてから対処することなどできない．社会的に許容される中でこそ可能であるが，結果として問題にされないという現状がある．それゆえに，自動車などはなぜ許容されているのかわからないと言われるが，結果論を安易に許容されていると判断すべきではない．安全において社会的に許容されているという前提を置くが，そこで事故データを使うとき，それが社会的に騒がれていなければ許容と判断する行為を犯してしまう．細かく相関付けていないから問題になりにくいと言えるが，人を殺すことを認める社会は成立しない．それゆえにそのような意図がないことにより安定が保たれていると考えられるが，加害者へとなることを避け被害者と対等であるためにこそ事前の立証が加害者（となる可能性を持つ者）によって要求されると考えられる．

２－２　機械の安全方策

国際安全規格において「隔離の安全」「停止の安全」という概念が背景にあると指摘（向殿，2003）される．しかし日本において一般的には，考え方の指針の提示といった受け取り方だと思われる．それ故に，この場合は「柵をすればいい」，「止めればいい」といった個別・付加的な対策を行ってリスク低減をするということになる．本論において，「安全に仕事をする」とは安全という概念を形成しそこを通して真と確信することである．故に，「隔離の安全」「停止の安全」という概念を通して真である状態を明晰化していく，つまり現実として具体的に作り上げていくのが設計と考える．概念の明晰化とは現実による制約の具体化である．

隔離とは単にガードといった発想が持たれがちであるが，人と危険源の接触が“ない”という状態として隔離という概念がある．人と危険源を離しその境界を指定したとき，「危険源が出ない」ということでの境界があり，また「人が入らない」ということでの境界がある．この 2 つの両立性（compatibility）としての具体化でガードがある．ガードが必要なのではなく，この 2 つの概念において真と確信することが必要であり，この場合ガードによって確信を得たとなる．「危険源が出ない」「人が入らない」とはそれが偽となる不可能性を示していくことになる．

また停止とは危害へとつながる可能性を無くすことであるが，“危険事象を生じるエネルギー（主に動力）が無くなること”が“可能性が無くなること”であり，“無い”という状態が停止である．ここでの「停止の安全」とは停止が完了した状態としての安全であり，停止トリガーが入ることではない．停止の完了を確認することで証明されるのが「停止の安全」である．

例えば，電磁ロック式ガード・インターロックは“停止の安全”ということに対し完全な体系と言えるかもしれない，しかしそれはガードとしての制約の検討抜きには語れない．ここにおける“ガード”は安全における思考フレームの具現化として認識する必要がある．先に述べたように，ガードがあるから内と外と二分できているかのように扱うのは間違いである．危険源を中心に論理として安全（外），安全でない（内）と二分する境界を見出していくときそれを具現化したのがガードや柵やカバーである．ガード等はその境界を具現化するものとして造られ，それ故に論理的に扱える．人に注意を促すロープを垂らしているだけでも同じように考えることができるかもしれない．しかしその時，そもそも安全として「人に怪我等は“ない”」ではなく，「人が怪我しようが何しようが頻度が下がれば」であり，その論理の領域は確率的前提である．怪我を前提としないということを確実にするのではなく，初めから怪我を前提としてそれを減らすとなると，それは「安全に仕事をする」ことの提示ではない．また，そのようなところでは，生産のためには怪我を許容するとなりがちである．確実にするということは隔離としての認識を一般的に共有できることである．

一般に工場における人間と機械のかかわりでは，2 つの安全があり，隔離と停止である（図 2-1）．現場において，「動いている機械を直接的に扱わなければならない」と言い，それ故にリスクと言うが，そもそも動いている機械を直接扱わなければいけないとしても，そこには「注意してやってくれ」等，そこに「こうやれば安全にやれる」という何らかがあるはずである．そこには隔離や停止の概念における仕事が見出せるはずである．そのような概念を抽出して「安全である」と確信しながら進むことができない仕事であるならば，「危険を安全に扱う」ではなく「危険を扱う」であり，安全を問題としないということである．

人の注意が安全の前提となると，危険を人に直接示すのがわかりやすいといった理由で作られていないだろうか．事故の後，安全対策が取られるが，事故の前に同じ対策を行うことがないのは，日本において人の注意が前提であり，注意が不十分であったので再教育を行うが再発防止の基本である．再教育で済まない場合に「技術的対策を取る」というのが日本における技術的立場である．そのような危険に対し，工学として初めての知見でわからないというわけではない．日本において，現場は最善の技術水準で構築されそう簡単にそれを超える技術的解答が得られないというかもしれないが，生産技術においてはそうかもしれない．しかし日本において技術とは生産技術であり，そこに安全技術は含まれない，または生産技術が優位である．

事故などの場合，事業者は労働者に対し賠償責任を負うが，無過失で賠償責任を負う方

が過失を争うよりも合理的な補償制度を作りやすいと言え，それは技術的方策（安全技術）と制度が結び付けられるが故と言える．日本では安全管理が中心と言われるが，本来管理するのであるならば技術の方が管理しやすく安全工学が必要とされると考えられる．技術的方策でなく教育による再発防止が取られるが，それは労働者が危険を引き受けるという自己責任論が通用してしまっている現状があり，安全教育はそれを強化する方向に働いていると考えられる．それが優秀な労働者なら事故は起きないという観念であり，それゆえ事故は人間のミスであり，また本来守られるはずの初心者および非熟練者の存在は曖昧になる．また，技術が責任を引き受ける構造でないが故に，機械システムは機能としての存在であり独立したシステムとしての自律性（安全確認構造）が持てないと考えられる．機械技術者は自らが提供する機械に事故を起こさせないということができない．

論理があるから考えることができるが，これは概念があるからモノを作ることができると言ってもいい．動く機械に接しながらも「事故が起こらなかったので安全」は，論理の後付けであり，「安全に仕事をする」ことに対し何ら証明性はない．機械に接するとき様々な場合があるかもしれない，しかし基本は安全の条件の中で扱うのであり，危険つまり怪我をするのを前提として扱うわけではない．通常の作業を決められた通りやっていても軽くはない怪我をし，あまつさえ死ぬこともあるという場合，その仕事を行うだろうか．「注意すればいい」と言われるが，通常の注意において怪我をする仕事が，確率が低いと許可されるのである．設計者・安全管理者は，自分では当然やらないような仕事でも，他人にやらせるのは問題ないのであろうか．もし，普通にやっていて怪我をしないのなら，それは安全が作られているはずであり，その点を明示すべきである．明示していくことで概念が明確になり，そこから論理的に，つまり安全として真であるということをいかに確保するか思考できるはずである．

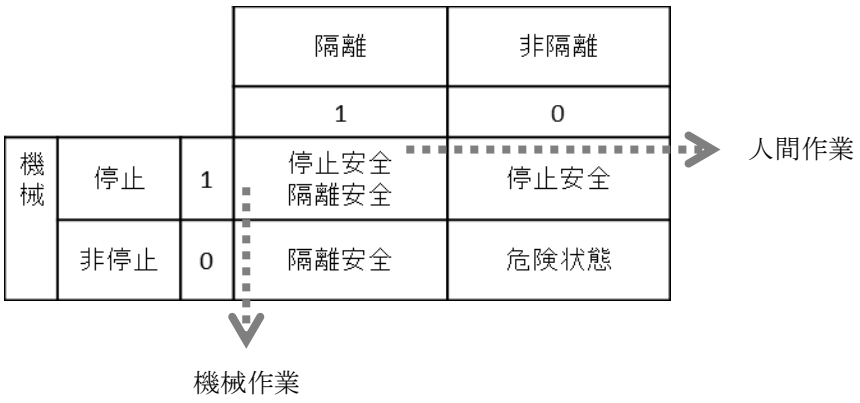


Fig2-1 作業における停止と隔離の切り分け

ガード・インターロックに話を戻すと，人間と機械の接触により事故が起こるとし，隔離（ガード）と停止の間でインターロックが行われる．図 2-1 のように，隔離（あり，なし）を論理（1，0），機械停止（停止，非停止）を論理（1，0）とすると，通常，機械作業（隔

離状態）と人間作業（停止状態）の切り替えとして（隔離，停止）が（1，0）⇔（0，1）となるように仕込まれる．これは隔離（ガード）と停止の 2 つの安全状態の切り替えについての論理であり，（隔離）∨（停止）＝１であることにより安全が保たれる．“作業する”とは「安全が保たれている中で行う」と言うとき，（隔離）∨（停止）＝１が成立している条件で行うということである．

当然ながら，ガードが閉まった（のが確認された）ので機械は停止を解除でき，停止が完了した（のが確認された）のでガードは開錠できるという関係であり，これは（隔離，停止）が（1，1）であるという過程を通ることを述べており，先の（隔離）∨（停止）＝１の論理を確保しながら切り替える構造である．ちなみに停止とは機械の完全停止であり，停止のトリガーが入ることではない．

極論として（1，0）⇔（0，1）と瞬時に切り替わるだろうが，それは開いた瞬間に瞬時に停止開始かつ完了ということになる．実際の作成においては，（隔離，停止）が（1，1）となる過程を通るのを求めるが，(0，0) にはなってはならないという非対称性で作られる．(0，0) は「停止していないのにガードが開く」，また「ガードが閉じられる前に起動する」という状態である．

ここで忘れがちなのは停止トリガーでもって扱うのは（0，0）の状態が存在しているということである．つまりこれは，止まったことによって切り替わるのでなく，止まる見込みでもって切り替わると言える．停止には時間がかかる．停止トリガーで切り替えを行う場合（つまり停止完了を確認しないということだが），この停止にかかる時間において隔離が論理０（非隔離）となることである．ドア開放に時間遅れ要素を組み込んだりする，または距離を取ったりすることで追加的な隔離を行おうとするが，しかしながら停止自体も遅れるかもしれない．つまり，安全と明言できないということである．通常すぐ止まるかもしれない，しかしすぐ止まるから安全ではなく，危険状態を過程として通るということを前提として考慮すべきである．

簡単に言うと，「開けたら止まる」（ドア開で停止トリガーが入る）は[（隔離，停止）：(1，0）→（0，0）→（0，1）]であり“安全でない”状態（0，0）があり，「止まったら開く」（停止確認でドア開のトリガーが入る）[（隔離，停止）：(1，0）→（1，1）→（0，1）]は“安全”な状態（1，1）を保つ過程である．日本ではインターロック装置というとこの「開いたら止まる」タイプが一般的に認知される．「開いたら止まる」タイプを使うことに問題があるのではなく，「止まったら開く」タイプが本来のインターロックであるという認識があるかどうかが問題である．インターロック装置の故障として危険側故障によりリスクが発生すると議論されるが，「開いたら止まる」タイプにおいては故障以前に危険状態を前提としており，「止まったら開く」は安全状態を前提としている．つまり，危険側故障として (0，0) となる確率やその時のリスクが計算され比較されるが，そもそも危険状態（(隔離）∨（停止）＝0）を前提としているものと安全状態（(隔離）∨（停止）＝1）を前提にしているものは区別されるべきである．そして，安全状態を基準として評価は考慮されな

ければいけない.（隔離）∨（停止）＝1 が成しえないとき，危険状態をどこまで許容するのかという論議になるが,「安全に仕事をする」ことにおいて（隔離）∨（停止）＝1 に対しどこまで整合的（integrity）かという問題になる.

一般に，安全側故障というとき，危険状態で壊れた機械が壊れているのに安全状態へ移行すべく働くのは矛盾した行為と言える．壊れても安全であるとは，そこに非制御状態での安全があり，そこへ移行できることである．それが一般に「止まる」であり，安全状態で停止したものを安全と認めないような社会的状況はそうない．よく航空機が止められない例に出されるが，しかし特殊な状況を取り出すことで，止まることを追及できる多くの一般の機械を止まらずにリスクで処理することで一般化すべきではない．リスクとするとき，人への危害に対しなんら制裁を受けない，また金銭賠償で済むという先入観がないだろうか．人の仕事を単純化するほど代替容易性が上がり，事故が起こった場合，機械に原因を求めると影響が大きいが，しかし人に原因を求めると，人の入れ替えで容易に再開できる．再発防止に再教育を行うという方便が通用するのも，個人的な問題に落とす故であり，それ故に人の直接または人心の入替である．人身傷害も保険料と人の入替コスト問題になる．労働者の自己責任意識があるからこそ可能な状態であるが，そもそも労働者の自己責任で労働現場の安全が保てないがゆえに事業者へ第一義的責任が課せられている．これは労働者の自己責任を強化するような教育の提供ではなく，職場環境・技術的解決を先んじることを要求するものである．安全方策・安全装置による安全確保が求められ，安全装置の故障は安全側（停止）となる限界としてのリスク評価であり，事故の原因は安全装置の欠陥に求めることである.

２－３　リスク

２－３－１　人間作業

リスクアセスメントにおいて,「どこまでやれば安全か」ということがよく論議される．そのような論議の中で中心なのは「どこまでリスクを下げればいいのか」という思考である．しかしここには,「よりリスクを下げれば，より安全」という素朴な信念がある．そして対処をすることでリスクは下がるものであり，許容可能なリスクに達するという思考である．そして，許容リスクは人間が受け入れるべきものであり,「受け入れたものについては人間の責任」という感覚もあるが，そこにおいて「人間がうまく扱うべきだ」という前提があると考えられる.

リスクという場合，ヒューマンエラーがよく取り上げられる．人間の信頼性を上げてヒューマンエラーをなくすという発想であり，また人間だから様々な適応ができるということで注意・警報に頼ることになる．人間は万能機械・部品であり人間はあらゆる作業に適応できるという前提がある．そこでは，人間の機械的評価でもあり，人間を機械と想定し

て，機械は劣化・故障するものであり，人間も同様であるとの評価である．しかし，人間がエラーしているという疑いはどこから出てくるのであろうか．エラーとは基準からの偏差でもある．基準が確かでないと評価はできない．なぜ基準（standard）が必要になるかというと，それにより可測（measurable）になるからである．完璧な Standard 人間があり，それぞれの人間は不完全だから事故を起こすのだとしたら，完璧な人間の仕事とは何であろうか．機械は故障するという評価があるが，例えばロボットアームはコントローラーが故障したから人を殴るのであろうか．問題は安全を確認しないからであり，安全条件における確認の完全性を確保しないからである．ヒューマンエラーとは人間を疑うものであり，その原因を人間特性に求めるものである．しかし，そこには人間はなかなか機械のように仕事ができなくて非効率という発想がないだろうか．

人間は「観察し予測する」ことを行っている．経験を積むとは，「観察し予測する」を体験により評価し改善していることである．人間に機械を委ねるとき，この「観察し予測する」は全て人間任せにすることで，安全を確保しない目的動作のみの機械を委ねている．そして人間が機械に組み込まれるとき，「観察し予測する」特性が奪われ，機械の部品となることで信頼性を上げることになる．本来，仕事とは“安全に”行うものであり，安全条件が定められるものであり，それを確認することでもって仕事をし，確認できないときはやめる（停止）ことで構成されるものである．この「確認」概念を正当に持つかどうかが信頼性と安全性の違いである．

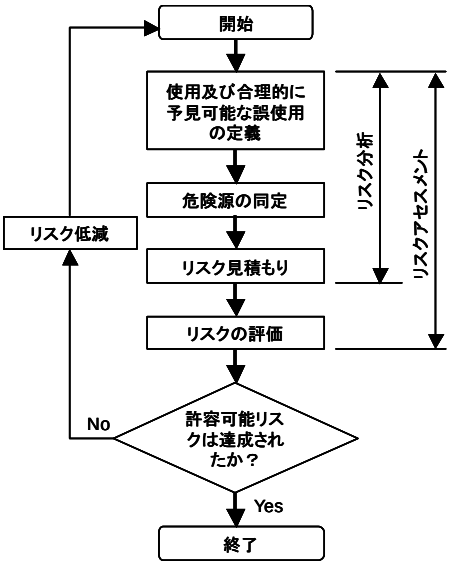


Fig2-2 リスクアセスメント

リスクアセスメント（図 2-2）の目的は「リスクを低減すること」ではなく「意図する使用」及び「合理的に予見可能な誤使用」の決定である．その判断基準が「示された仕事が許容可能であるか」である．労働者は「安全に仕事をする」のであり，安全という概念が真であるという確信でもって作業を行う．この「“安全に”を“確認”する」が配慮されないリスク低減はどんなに下げたところで，そもそも下げる基準が違うと言わざるを得ない．

信頼性基準で下げているのであり，安全性基準で下げてはいない．そもそも日本では，信頼性でも安全性でも，結果として事故が起こるのならどちらでも同じという認識がある．結果主義であり，それゆえ結果としての被害の大小で比較すればいいとなる．

本来として「意図する使用」及び「合理的に予見可能な誤使用」と定義されたことにおいて「安全に仕事をする」が真となる．当然，「意図する使用」において，意識して仕事をしているとき安全が確保されるが，意図しないときすなわち“やめる”（受動性として停止する）ことにおいても安全は確保される．また意識の正常性が保たれていないときも受動的に安全が保たれることが求められる．これらは，一旦止まるようなことができるからこそ，迷ったり考えたりができると言える．そして「合理的に予見可能な誤使用」が「意図する使用」を基準として合理的に検討されるが，その逸脱において抑止的に停止（可能性を無くす）や制限（超えることの不可能性）といった，使用者が受動的に為す制約を設けることになる．簡単に述べると，手順を違えると停止する，構造的に違う組み合わせで組めないといったことである．

ここには，危険源から離れている（隔離），“やめる”ことができる（停止）の概念が垣間見える．人間だから柔軟にやれるというが，その通りであり，「隔離の安全」「停止の安全」という概念でもってそれが真となる状態で仕事をしながらも，機械に比べてその設定を柔軟に行っていると言える．しかしこれは人間だから安全を無視できるという柔軟さではない．すなわち人間においてもインターロック構成でもって仕事をしているということであるが，人間こそインターロック構成でもって仕事をしており，それを機械が模倣しているというほうが適切である．安全という概念の中でその概念の中に在るという自律性があるからこそ，安全は真であるという認識を持ちうる．そして“やめる”ことで安全な領域があり，自律性を逸脱する前に “やめる”という判断を行いうるということこそ，自律性の限界としてのインターロック構成である．

リスクアセスメントは「安全に仕事をする」ことから逸脱しやすい仕事の定義においてそれを許容できるかという問題である．「意図する使用」が狭まればそこを逸脱する可能性も高まる．そうなると「合理的に予見できる誤使用」において止めるのに間に合わない，制限を超えてしまうということでリスク状態となる可能性も高まる．「安全に仕事をする」このことを基準にして，その基準からどのように離れてしまう仕事が構成されるか，その仕事を労働者が許容できるかという問題である．実際問題としてリスクが大きいので下げるということをやっているように見えるかもしれないが，許容可能な仕事の設計を行っているのであり，労働者がその危険を安全に“扱いうる”という判断が許容可能である．“扱いうる”すなわち制御可能と判断するが，制御主体としての人間の判断であり，その制御の失敗を評価しているのがリスクである．

２－３－２　リスク評価

国際安全規格は，リスクで考えるとして共通化しようとしている．人と危険源の関係として主に述べられ，人が危険源に暴露されることにより危険状態になる．確かに“安全”としてではなく“リスク”として共通化しようとしているが，これは“安全”ではなく“リスク”で考えるということではない．安全が個別具体的に形成されていく中で，その安全を逸脱することの評価としてリスクを考えるということである．

「安全に仕事をする」においてそこで持つ概念を通し安全が真であると確信して実行するが，裏を返すとその確信の度合いという問題になるという前提である．確かに確信の度合いが低ければ，そもそもなぜ確信しているのかという疑問が生じる．また度合いが高ければ良さそうに感じる．そして安全が偽となる評価が確率的になされ，そのときの被害がリスク評価される．確かに，安全の概念の形成において結果として生じうることをリスクとして考慮すること（小さければいいというわけではない）は必要である．しかし，リスクを考慮すればそこに安全の概念が形成されているはずとは言えない．国際規格においても方法論（３ステップ・メソッド等）を通した結果としてのリスク評価であり，リスク評価から逆にたどるものではない．

リスクとして考えるにしても，リスク自体を共通の数値として扱うのには留保すべきである．リスク＝危害のひどさ×発生確率としたとき，例えば危害のひどさ[4]×発生確率[2]でも危害のひどさ[2]×発生確率[4]でも同じリスク[8]であるが，これをもって片方を許容するならもう片方も許容すると考えることはできるのだろうか．産業安全におけるリスクとは保険からきている．産業事故における損害賠償としてのリスク管理である．工場においては安全管理が行われていたが，そこで起こる事故・傷害等においてその損害賠償を経営的に管理せざるをえないという状況においてリスクマネジメントが発展してきた．損害賠償は特に他の方法が指定されなければ金銭賠償で行われるのが基本になっている．金銭で行うとき，先のリスクの中身が違っても結果として手当てする額が同じなら区別がないということであり，リスクを下げる方向に管理を行うとは金銭的コントロールである．リスク管理部門においてはリスク（金銭賠償・保険の査定）を下げることを目的とするであろう．そのとき，10 人の指を 1 本ずつ飛ばすより 1 人の指を 10 本飛ばす方が金銭賠償額は小さいとした場合，または設備停止による損害よりも人の死亡の方が金銭負担は小さいとした場合，安全管理はその方針で行うべきであろうか．

規格にはリスクアセスメントにおいてその方法論（本質安全設計を優先等）が示されている．また法規制も存在する．リスクマネジメントの評価によって方法論や法規制が無視されるようなことが感覚的には了解されるのなら，その社会において方法論や法規制は構成的な意味を成すものではない．すなわち，制度を作っていくことで社会を作っていくのは制度に構成的意味を見出していくが，社会というものがあるのでそこに合うなら制度も

認められるという関係であれば構成的ではなく，社会とは無関係の制度であり社会を構成する制度ではない．歴史として，日本において唐を倣って律令を導入したが，日本に合うものの取捨選択であり改変である，日本としてその中身はこれまでと変わらないが近代的な衣を身に纏うというような行為である．江戸時代末期の不平等条約において，「近代的法体系がないところでは権利が保護されるのかの予測がつかない」というのが治外法権の理由であり，その撤廃へと明治時代において近代国家としての体裁を纏うため各国の法を検討し導入を行ったが，不平等条約は撤廃できても（法整備より軍事的自立の意味合いが強いが)，「法の遂行者による支配」ではなく「法による支配」が実現されたとは言えない．法以外の何者にも支配されないことを実現するにはコストが必要であり，例えば行政組織の対立的多重化は単純に 2 倍のコストと考えてみても，コスト評価だけで一重とするとはならない．もしコストで選ぶとしても，一重だがチェック機関の独立性等を検討したりする．ここで考えなければいけないのは，この場合の一重は選択肢ではないということである．一重が選択肢で“ある”か“ない”では意味が全く違う．一重は機能としての説明であり，その機能にどのような問題が生じるかを考えるとき，一重は単純な選択肢ではない．

制度（法など）において新たな決まり等を導入するとその矛盾は社会的に現れてくる．社会に現れる矛盾をどこまで考慮できるかは重要である．しかし影響が現れない制度なら導入するというのは，そこでは結果に意味があり導入意志は意味を成さない．悪い意図であっても，結果として社会的影響が生じなければ問われることはない．結果が行為に先行する社会において，行為とは関係性で決まり個人の内面性ではない．故に自身が行為主体であると自覚することもないと考えられ，結果責任を追及するは，責任を感じない人を無責任と責めることに陥る．また，無責任な人が事故を起こした人を無責任と責めるような構図でもある．

リスクは行為における決意の論理である．可能性の“選択”による分岐であり，概念的非対称性である．原因として関与することであり，結果しか見ない者にとってリスクは不要である．結果を見ることでしか理解しない者にとって，概念を持つ必要はなく，コントロールは不要である．その者は「結果として実現すること」が理解可能なことであり，結果を避けることにおいて，（避けると）「実現しない」がゆえに関心は持てないと言っていい．リスクにおいて，そこでは完全でないがゆえに確率的に様々な可能性が重畳することを認識する．それは目を通した物理的認識ではなく，概念を認識するメタ概念的ともいえる．例えば，機械作業者は事故という結果を見て非常停止を押すわけではない．また“事故なし”に賭けているわけでもない．常に実行・停止の判断にさらされながら，「停まれるが，まだ停まらなくていい」と実行を決意（判断）しているのが機械の運転状態である．その実行の中で操作の選択を行っている．急停止に近いほど停止時に生産物を破壊するかもしれないがギリギリまで生産性を高められる．十分に余裕のある停止において生産物は維持されるが，生産時間が減少したりする．ここでは推論における選択（停止 or 実行）を

行っている．単に機械作業において失敗する・しないで評価している者は，そこに主体的判断もコントロール意思もなく，結果のみが関心事である．

リスクアセスメントにおいて，①主体である自身の正当性を立証するのか，②社会への影響を及ぼさないことを立証するのか，どちらに主眼が置かれるのかの違いが表れてくる．リスクアセスメントは行為が及ぼす結果可能性を評価するものである．結果主義は結果に責任を持つが，結果が全てとなるとき，行為に責任主体はなくなる．そのようなとき②が全てであり①の意味はなくなる．行為主義も極論となれば行為が善ければ結果を問わないとなり①が全てで②の意味はない．

個人の確立が重視されるところでは①が重要であるが，しかしそれでも社会的存在である以上②を考慮しないわけにはいかない．このような関係が妥当なとこなのであろう．リスクアセスメントは因果的形式（原因→結果の方向性）で述べているのみで，結果が行為（原因）を規定することはない．つまり，結果（リスク）が示されるが，「その行為を受け入れるか（許容可能か)」とは聞いても，結果が小さいことが正しいとは述べていない．正しいと思う行為を，その結果が受け入れられるなら実行する，という形式である．

２－３－３　リスクコミュニケーション

リスクアセスメントにおいて人と危険源との関係において，その相互性が検討される．危険源がないと知らされれば人にとっては安全であり，人が居ないと知らされれば危険源（機械）にとってある意味安全である．リスクアセスメントにおいては相手との関係であり，前節のリスクアセスメントも人の作業に注目したがそれは危険源との関係で定まっていく．

相互性とはコミュニケーションの問題と考えていくこともできる．許容リスクに下がったかどうかのコミュニケーションではなく，使用者が危険源との間でコミュニケーションを取れるかどうか，つまり危険を認識し安全に扱えるかどうかという問題である．そして，このことの使用者における納得について設計者とのコミュニケーション問題がある．

コミュニケーションにおいて送り手と受け手の関係であるが，立場を入れ替えた相互性がある．この送り手・受け手は通信機（communicator）のトランスミッター（transmitter 送信機）とレシーバー（receiver 受信機）として見れば，感傷的視点を排除できると思う．レシーバーが無ければ，そもそもトランスミッターは送信の動機がない．レシーバーの能力でない周波数，通信速度，また，レシーバーが解析できない信号情報も意味がない．トランスミッターに合わせたレシーバーを要求するかもしれない，しかしレシーバーによって通信は成立しており，レシーバーの能力が基準になる．トランスミッターは通信を開始するかもしれないが成立させるものではない．ここで述べたいのは，コミュニケーションは受け手によって成立するということである．送り手（話し手）が何を喋ろうと受け手（聞

き手）が居なければ，または聞かなければ，または理解できなければ，成立しない．設計者がいくらリスクを下げたと言おうが，使用者が危険源との間でコミュニケーションを取れるか，つまり危険源を認識しそれを理解して対処を行うことができるか，このことが解決されていなければ，低リスクが受け入れ可能という問題にはならない．現状としては，送り手が受け手に理解することを要求しており，受け手の能力を超えてのコミュニケーションは成立しない．

使用者は“受け入れる”ということで解決できるが，設計者・製造者が“受け入れろ”ということで解決はできない．つまりコミュニケーション成立の問題ではなくなる．社会的受容性が高い社会とは市民つまり受け手の能力（理解力，判断力）が高い社会であり，使用者が扱いうるという判断を使用者自身で理解してできる社会である．それゆえ市民教育が重要性を増すのは，高めた分だけ受容可能性が増すからである．送り手側が自分たちの制約（受け手の能力）を理解しないとしたら，それはコミュニケーションの問題ではなくなる．市民に知らせなければいい，理解できない市民に問題がある，理解できないのなら知る必要はない，結果としてリスクが小さいと出ているのでそれを受け入れればいい，というところにコミュニケーション的解決がないのは明らかだが，コミュニケーションに解決を求めていないのならリスクアセスメントではなく別の手段を取るべきである．現状，日本における製造者等にとってリスクアセスメントが“やらされる”ものでしかない状況において，コミュニケーションの動機付けは生じていない．

専門家の役割は市民とのコミュニケーション（通信）を成立させることへの働きかけであり，市民のレシーバーとしての回路調整・デコード処理能力の中にトランスミッター（製造者の説明能力）の能力を入れることであり，また市民の能力に対して助けることであり，アップデートしていくことである．市民の主体性を助けることで市民が自身で判断する能力を拡大することが，市民社会で求められる専門家の役割である．つまり，市民社会を耕す（cultivate）ことにより形成されているものが文化（culture）である．

例えば，インフォームド・コンセントについて考えてみる．簡単に「説明と同意」と訳されるが，日本では「医の倫理」問題で取り上げられ，それ故に医療分野の問題かのように限定されがちである．ここで問題となるのは患者の自己決定である．自己決定を行うとは主体的な存在であり，決して従属的ではないということである．医者は患者が自己決定を行っていることを確認してこそインフォームド・コンセントを行ったと言える．医者（トランスミッター）は説明の受け手である患者（レシーバー）に説明を行い，患者はそれを理解し，患者（トランスミッター）は同意の受け手である医者（レシーバー）に同意を伝える．このとき，医者は送った情報ではなく受け取った情報の中に，自律性・知識・理解・判断能力としての同意を読み取れる（2 番目のコミュニケーション成立）ことによって最初のコミュニケーションが成立したことを理解する．極論すると，インフォームド・コンセントは患者による説明に対し医者による同意によって成立する．

設計者が意図した危険源と使用者の間でコミュニケーションが成立したことを，設計者は確認できているのだろうかということが問われる．ただし，同意と言っても患者・使用者があらゆる責任を引き受けるというわけでもなく，また医者・設計者が全てにおいて免責となるというわけでもない．幻想的な期待を排除することであり，互いに選択する苦しさへ引き込むことである．帰結に従うことではなく選択することを条件づける基盤に置くことであり，安心することでなく自由（不安）に置くことである．

２－４　小括

ガードは環境的制約の固定化であり，ガードが閉じていれば中で何が起こっても構わない．どのようなやり方であっても，停止を確認したらガードを開ければいい，と単純化できる．欧州の機械安全はガードを前提にしたイメージが強いが，日本においてその前提はない．それゆえ，設計自体がガードを前提とするものではない．リスクアセスメントで問題となったらガードを付けるという理解であり，（元々の設計がガードを前提としていないため）多くは生産のことも考慮するとガードを付けられないから，リスクを許容せざるをえないというのが実際である．使用者がリスクを引き受けることがリスクの考え方であると誤解させるところがあった．それは，ガードを付けないことがリスクアセスメントによって正当化されるということになり，リスクアセスメント（リスクが小さいという結果を示すこととして）を行えば安全問題は片が付くとなった．事後においてトラブルが様々あり，行政的判断や裁判があるが，リスクアセスメントが常識となる中，リスクアセスメントがなければ裁判に負けるという認識はできつつあるが，逆に，リスクアセスメントをすれば裁判に勝てるという誤解もある．そしてその誤解により逆に，リスクアセスメントをすると免責になるからと広まる流れでもある．本来の趣旨に反し，トラブルを起こさないためでなく，後のトラブルを解決する手段として，また，使用者と製造（設計）者の間で安全問題を解決するのではなく，事後に PL で欠陥でないと認められるためとして，つまり被害者の救済を行うためでなく無関係となるためと理解される傾向がある．

日本では「安全である」のが「当たり前」であり“安全”と言わなければいけないという状況があり，リスクを引き受けてもらうという交渉が行われにくい．それゆえ，リスクアセスメントにおいても，リスクが残るとは言えず，リスクアセスメント（危険分析）により“安全”と言わなければいけないという，ねじれた状況がある．許容リスクという社会的合意性の形成が無いのに，有るかのように振る舞いそして有るかのように錯覚してきているのが，リスクアセスメントをすれば安全であるとする，日本における理解である．

本来，ガードで完全に覆ったものに対して，一部のガードを外すことによりリスクが現れてくる．そして，そのリスクは扱えるか，扱えないならガードを外せない，という交渉がなされる．しかし，ユーザーが危険な機械を使いこなすのは当たり前という感覚が設計にまであり，そのような交渉はなされない．はじめから人が危険を注意しながら扱うこと

が前提であるとは，剥き出しの機械において膨大なリスク評価項目が出てくるということになる．それゆえ，リスクアセスメントは困難になる．

機械安全成立時と違い，新しい機械として「ガードという環境固定的な方法はとれない」仕事としての要求があり，そこにどう対応していくかという問題として，製品安全や機能安全といった拡張がなされている．それはガードという環境に対し固定的な方法ではなく，変化する環境に対し均衡を取るような方法を検討するということである．単にガードを付けられないからリスクアセスメントをすればいいという問題ではない．また，信頼性とは耐えるといえばわかりやすいが，環境への積極的介入は行わずに耐えることができるかという問題であることが多い．多くは目的に対する機能であり，それが環境に耐える信頼性である．一般的に環境自体をそう変化しないように作るため，環境変動の多くは人によるもので，日本ではこれまでガードを付けなくても“人の注意”とすることで機械の問題では無いことにできた．しかし例えば，人と機械の協働という場合，人の注意に期待するという相互性を求めても，複雑に動作する機械への注意の確保は難しい．そもそも作業に集中するということは，それ以外の注意がなくなることである．このことは，人が機械に対し注意するということは，他の作業（本来の目的）を行えないということである．これは，機械において積極的に自らの環境条件へ関与していかなければ安全が確保されないのは明白である．機械において，目的機能ではなく環境に作用する機能としての安全への関与が求められる．

“安全でない”を前提とした論理性は見出しにくい．あくまで“安全である”ということに論理性があり，“安全である”ということが必ず真となるような状態を確保するというところで各状態の整合性を求めていくことしかできない．機械においてもその“安全である”状態を確保していくことこそ環境的介入作用であり，安全機能の理解である．リスクとはその“安全である”の確からしさと表現しうるものである．リスクでは機械と人間が接触することで事故へとつながるとするが，接触過程という相互性が現れる前にそれぞれにおいて安全構造があり，その逸脱においての相互性である．つまり結果として「(衝突する）相手がなかったら何も問題なく，相手があるときだけ問題となる」のではなく，「相手がいないこと」の確信（確認）をもって行為を行っているかという問題である．機械も人もその存立において自律性を持つ構造が自己インターロックとして表現される．

リスクを人と危険源との関係において考えるに当たり，リスクアセスメントにおいて機械及び人を取り上げ考察したが，リスクの前提になる概念があり，技術者や安全管理者はリスクで安全対策を行うのではなく，安全対策を行ったものをリスクで評価するという関係である．

“安全”として完結するという論理があり，その論理との一致に証明性があり，そこからの差異に評価がある．「隔離の安全」「停止の安全」とあるが，必要なのは安全という概念を明確にすることであり，そこを通して確認することで安全において真であると確信を持つインターロック概念がある．自身の安全に責任を持つということは，自らの正当性を

自ら示すことであり，機械も人も安全を確保し実行するという自己インターロック構造として表される．そしてそれは“安全が確認できなければ止まる”というところに作業または機械において共通性を持つと見るべきである．

第３章　不安の概念と停止

３－１　事故を防ぐ操作としての安全

「安全」とは，何となく，信頼性を上げて事故の不安を解消することだと思われている．ここに「安全を不要とするほどに信頼性が高いことを安全という」というようなトートロジが生じて安全の権威のなさを思わせる．安全とは無関係に権威づけられた“安全確認”が，例えば事故後の再稼働のためになされるのであるが，危険が生じたらいつでも停止できるシステムを要求する最も重要な原理（安全確認の原理）をむしろ否定するような“安全確認”がなされて，そのことで却って，事故の可能性が作り出される．このように，安全の権威のなさが，明らかに，私たちの国の安全問題を象徴すると思えてならない．

事故は自然には防げない．回避するとしたら，回避の目的を明確にして，そのための情報と操作を制御として実行すること以外にはない．しかし現実には，この操作は必ず成功するとは限らない．そのため操作の結果を確認する必要があるが，ここで重要なことは，確認できないとき停止して少なくとも事故の可能性を一旦遮断することである．特に重大な被害が予測される場合，この「停止」は絶対的条件でさえある．安全確認の原理に準拠して「安全」は２値の論理で扱われるが，それは，“安全”／“安全でない”を明確に区別し，回避の失敗で生ずる“安全でない”に対して必然的に「事故の前に停止する」を保証する．事故を回避するどんな約束も，結局事故の前の停止の保証なくして正当な「安全」と認めてはならないなのではないか．致命的とされる被害が予測されるシステムでは，計画に当って，安全を，確認される安全（合目的的安全）と停止（無条件安全）の 2 値で表し，事故の可能性を完全に排除して安全が確定されなければならないとされる．

一方，被害が致命的でないと言える場合，「リスク」の適用が可能である．EU の CE マーキングのような社会制度を前提とするが，私たちの国の不法行為法（民法 709 条等）では回避の失敗による事故の被害が金銭的賠償によって修復可能である場合に限りリスクの論理が適用される．危険の予見と事故の回避義務の限りを尽くし，さらにリスクアセスメントによって許容リスクレベル（賠償による修復可能の条件）をクリアして「認証」の要求に誓約書（文書化）をもって応える．このことは，事後の責任（被害の可能性）を明確にして，社会の混乱を生じない準備を整えた製品のみ市場に受け容れるというリスクベース社会の考え方である．このような社会では，被害を小さく抑えることがリスクの考え方を共有する条件となっており，CE マーキングは，前もって認証を得た商品に対して EU 域内の流通を許可するという事故の予防原則の適用を図る欧州の自由貿易の政策である．

３－２　リスク低減と安全の条件

ところで，死亡事故や原発の過酷事故のように金銭的賠償が予定できないような致命的被害の可能性が残る場合，リスクの論理（被害の期待値に対する事前の説明責任の論理）は通用しない．もともと事故の中には，“取り返しのつかない”と言える被害が存在している．誰もが承知していても，経験すること自体が許されない深刻な事故のことである．取り返しがつかない以上，確率が小さいから事故を許容するというわけにはいかない．あるいは，起こってしまった後で結果論を持ち出し，大した被害でなかったと言訳けし，場合によっては，責任の一端を被害者（死亡者）に押し付けてけりをつけるという暴力的やり方は言語道断である．

確率論に頼るのは，「停止」による安全が確保されていないためだが，本当は，確率論的問題が残ること自体が問題なのである．安全問題は，問題の本質が“そこ（確率論に依拠すること)”にあることが認識されていないために起こっているといっても過言ではない．安全の確率論的曖昧さを遮断できるのは，「停止」の構造的保証（クリティカル・インタロック）だけである．停止不在の構造を深刻な欠陥と見ていないのは，犠牲の大きな事故であっても深刻な事故と見ていないことの証拠である．安全の立場からは，「止まる」操作の妥当性ではなく，事故の前に「止まる」ことの完全性を求めるべきである．ベネフィットを主張して初めから諦めるのでなく，安全の絶対的要求に応えないわけにはいかない．

事故とは何であろうか．事故とはあまりに主観的で定義するのは不可能である．強いて，制御の立場から共通化を試みると，事故とは，停止を絶対的に要求される事象だということであろう．確かに，事故を起こすと停止を強制される．自動車事故ではそれでも停止しない場合は“ひき逃げ”となって，絶対に許されないという状況を呈する．そうなると，事故を防ぐというのは「事故」の前に止まることだということになる．安全は，実行してみないと分からないというわけにいかないから，いざという時，確実に停止できることが予め証明されなければ「安全」とは認められない．安全は，本質的停止構造（後で示す遮断停止）としてノーマル・クローズタイプの電源やブレーキが使用される．

リスクは，あくまでも被害を小さいと見て事故を受け容れるための合意を得ようとするものであり，したがって結果責任の影響を避けるため，少なくとも取り返しのつかない事故（死亡事故は当然）は除外しておくことが条件となる．リスクアセスメントは残留リスクにおける責任能力（賠償による原状復帰の保障）に対する事前の承認を得るために行うもので，改めて，「認証」とは，取り返しがつかない事故の可能性を事前に排除しておこうとする社会システムだと理解できる．私たちの国のように認証を制度としない国は致命的事故を覚悟せざるを得ないが，そのために何らかの解決策を持ち得ているのだろうか．結果論で処理できるとなれば，取り返しのつかない事故など“ない”というのと変わりはない．私たちの国では賠償では取り返しのつかない事故を補償（結果責任保険）で「償う」というやり方が慣例化・儀礼化している．起こってしまったことは仕方がないとする結果論で，取り返しのつかない事故もお金でケリをつけることが可能だとすれば，保険で予定するなど，死亡事故を「取り返しのつかない事故」などとはじめから考える必要がない．

安全に対する予防概念（事前責任）がこれまで私たちの国では曖昧であったこと，そして，今後ますます結果責任の軽減化(寛刑化)が進み，安全の予防の目的が失われていくと危惧されること，このことから結果責任のままにそれを避けるためのリスクと確率論の適用には見直しが主張されなければならない．

リスクは，被害が小さい事故を受け容れるための合意（利便享受する立場での契約）に係わることであって，リスク低減は，事故を防ぐとする本来の「安全」とは目的が異なる．制裁を含んで高額の補償に困惑した PL 訴訟の経験からの対策(米国)もあるが，大きな被害を排除して事故に対する責任能力（予防とその限界で生ずる事故の賠償能力）を個々に宣言して認証を受けるという制度が欧州を中心に展開されている．社会的混乱を未然に防ぐ目的を理解して，リスク低減による事故の予防を略式の安全と認めることができるかもしれない．

リスクの立場から絶対安全はないと主張されるが，リスク低減は，事故を防ぐという目的はもともと持っていいない．とは言え，事故はあくまでも防ぐべきことであり，少なくとも予測／回避を必至と考えるべき取り返しのつかない被害は制御に頼る以外にはないと考えなければならない．

３－３　不安の構造

“不安を停止とする”とする機械の安全原則（杉本，蓬原，1990）を適用しないまま危険回避を人間に強いるような特異な人間機械系が実施されている現状がある．割り切って絶対安全はあり得ないとするのはリスクベース社会の基本姿勢である．安全には曖昧（不確実）が残るために必然的に生ずる不安をリスクで表し，社会的に広く容認されるレベル（許容リスクレベル）を達成して安全と見なそうとするのは国際安全規格 ISO12100 に基礎を置く考え方である．このように，「リスク」は，安全に含まれる不安の指標であるが，受容リスクと言うとき，そこに自らが扱いうる不安であるという感覚がある．日本でいう「安心」には「関係なくなる」という感覚があり，リスクベースの安全における主体性とはかけ離れたものがある．安全は予測過程を扱う．リスクベースはコントロールの主体性を扱っており，安全の予測の構造を要求しているのではないかと考える．

一般に，安全にはルールが作られる．事故を防ぐためにやるべきこと，やってはならないことが規定され，事故が起こるとルールが原因と責任の根拠を与える．安全に対する不信感は，事故は絶対には防げないとしながらも防がなければならないとする私たちの国の安全文化の後進性にあると思われてならない．リスクベースの世界では，事故（Accident）は衡平に起こり，負うべき責任も衡平である．この衡平性を担保しようとするのが実は安全のルールなのである．

しかし，衡平を原理としながらも安心に至るのは難しい．現実にも，許容リスクレベルを達成しても不安は容易に解消されない．リスクの中に許され難い危害（the critical

injury）の可能性（端的には経済的損害とする定型的な処理では済まされない）が残る場合である．この可能性には，無関係の弱者，幼い子どもが被害を受ける場合が含まれる．このような場合，リスクを低減するというよりも，当該事故を予測して，確実に（確率に頼らない方法で）回避するという安全特有の制御の課題（例えばフェールセーフの採用）となることは明らかであり，そして，制御による安全（事故回避）には失敗は決して許されない．

３－４　リスク受容と不安の本質

一般に，「ベネフィット」を求めるものが，引き換えに「リスク」を受け容れるか否かを判断する．リスク受容を判断する場合，取り返しのつかない致命的被害は起こり得てならないから，リスク受容の判断の対象から除外されると考えて当然である．端的に言えば，リスクで扱われる被害は，定型化された補償の手続きで処理可能な程度(severity)に限定されると考えていい．

日本では，安全は合理的理由を以て「無事」と認めること，そして「安心」は心理的なものであるが，また安全だと勝手に思い込んでいるに過ぎないとする見方もなされる場合がある．安心はセキュア（secure，ここでは「心配事がない」という意味において）と比較されうると考える．ここで「心配事がない」とは 2 つの意味で考えることができる．それは，

自らコントロールできていると確信すること，

または，自分には関係ないと確信すること，

の 2 つである．そしてセキュアは前者の意味合いが比較的強く，安心は後者の意味合いが比較的強いといえる．不安の残るような安全は本物でない可能性がある．しかし不安を無くすということは，先の安心・セキュアにおいて無関係とすることは“油断”となる危険性があり，また不安を完全にコントロールできるという“過信”に陥る場合もある．低リスクであるとは，表現を変えると，危険を確認するという行為によって自らの正常性を確認している状態と言うことができる．低リスク（受容リスク）が安心・セキュアであるとは，「不安の時は，危険の可能性のある行為をいつでも停止できる」とする関係が正当であり，いつでも「やめること」ができるから“不安なく”実行することができるという関係である．

何かを判断するとき，「A か，B か」と行われる．A という可能性か B という可能性か，どちらを選択するかと．そこでわからないときは“安全側に”と言われる．“安全側”に非対称な選択のためにリスク評価等が行われるかもしれない．しかし，“わからない”は A か B かではなくそのような選択をしてもいいかどうか，そのもの自体もわからないという場合もある．つまりそこには，“やめる”という無対称（non-symmetry）とでも言うべき状態があり，それ故に“やめない”という状態の中で選択が行われる．そして“やめる”とい

うところに確定性が必要になる．いつでも“やめる”ことができるから，“やめない”という判断の中で，他の選択ができる．

安全とは安全条件に対し合理的に安全が確保できていると「わかっている」ときに実行がされるものであり，「わからない」ときに実行するものではない．このとき“やめる”ことが確定されているからこそ，つまり“やめる”ことによりリスクのない状態があるからこそ「安心」することができる．安心とは「わからない」ものに対処をしなくていいと確信することであり，それ故に「わかる」中においてコントロールしていくことである．コントロールできるとは，どこまでリスクを上げられるかであり，それは「やめる」ことによりリスクがないという状態があるからこそ，そこから上げていくことができる．つまり，機械はリスクが発現する前つまり事故の前に“止まれる”という条件の中でこそ実行できるのであり，実行している機械を“回避”や“止める”ことでリスク低減するのではない．

リスク受容は，単なる「リスク」でなく，不安を考慮して次のような判断がなされていると考えられる．

① 被害の発生確率が小さいことで判断する．
② 事故の回避の一部を担当する場合，それが容易であることで判断する．
③ 事故が予測されるときいつでも停止できることで判断する．

いずれも，判断には，自由／独立，「拒否」の権利が前提であり，③は不安（不信）の時はいつでも停止できるから安心であり，そういう安全が真に安心を与えるというのは図 3-1 と表現できる．確かに，ブレーキを持たない自動車のように一旦走り出すと止められないようなシステムはもともと安心できるはずはない．

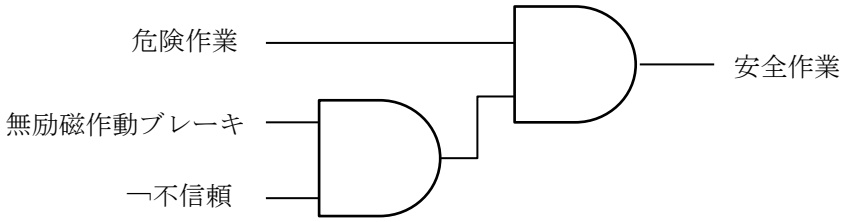


Fig3-1　インターロック表現

ベネフィット享受の主体者がリスク受容の判断を主体的に行う．リスク受容を判断している限りは，リスクの現実である事故（被害）の責任を均しく負うということになる．メーカーの安全配慮義務（民法 415 条，710 条，PL 法等）に対する衡平性，すなわち，安全配慮義務をメーカーが完全には遂行できない場合，リスクを受容すると判断する限り，義務の代行を引き受ける側にも平等（衡平）に負うべき責任があると考えなければならない．衡平責任が曖昧であるため，私たちの国では，リスク受容に依然として残る「不安」は，事故の責任に対する事前の対応が難しいことで生じているのではないか．「事故はメーカーの一方的責任だ」，逆に，「リスク受容によってメーカーの責任は完全に免除されて当然だ」と考えたりする曖昧の中で生ずる不安だと言える．

リスク受容を可能とするには，経済的損害として扱うことができない事故を排除しておく必要がある．そこで，責任（被害の救済・補償）を衡平に負う目的でルールが作られる．安全に関する法規格はそのためにあると言っていい．事故の責任が広く整合されたルール（国際規格）で定型化（制度化）できれば，事後の裁判を待つまでもなく，予めルールに準拠して認証マークを取得することで，例えば安全配慮義務を果たしているかどうか確定できる．明らかに安心を得るシステムである．State of the arts で到達した技術を共有する関係は，事前において，事故（Accident には偶然の意味がある）を経済的被害と認め合う合理的な関係を前提としているのである．

一方，私たちの国においては消費者(ユーザー)の衡平な責任分担を制度として取り入れるのに困難している．私たちの国では，業務上過失の考え方があるが，それがメーカーであるかユーザーであるかは事故の状況から判断される．PL 法においては，事故の第一義の責任（欠陥なしの立証）はあくまでも製品の欠陥に因るとされる．しかし無欠陥であることはなく，どの程度の許容範囲があるかという問題がある．本来，事故の被害者はベネフィットの見返りとしてリスクを受容したのであって，負担の大小は兎も角として，事故の責任を，一方的にメーカーに負わせるのは正義だとは言えない．しかし，この関係が事故の前に問われることはない．

特に注意を要するのは，この契約外の第三者に被害が及ぶ場合である．致命的被害に巻き込むことは絶対に避けなければならない．彼らは，ベネフィットにもリスクにも関わっておらず，責任ある自律した立場，拒否する権利とは完全に無縁な立場である．何も知らないまま被害の対象とされていることになる．公害など製造者と消費者の利害の外における地域住民に起こっていることで，利害調整において完全に無視されていた歴史である．自動車においても，歩行者とは車対車と違い第三者性があるが，車に対抗できるわけもなく一方的な被害である．このような場合，加害者に多額の補償責任が課せられるが，そのこと以前に，失敗が許されない条件で回避すべきとする制御の対象であることは明らかである．このように，安全には，リスク受容としての契約関係を確保するという条件で守られる安全と，契約とは無関係の第三者に与える被害に対する安全とに分けられ，これらは明確に区別される．

３－５　不安のカテゴリーの生成過程

現実に，許容リスクレベルを達成しても不安は容易に解消されない．リスクの中に許され難い危害（the critical injury）の可能性（端的にはお金による補償では済まされない）が残る状況である．例えば，自動車の場合，メーカーの責任で運転士の安全が守られるという前提で，自動車の利便性を考えてユーザーがリスク受容を判断する．関係者間の衡平性に関わる契約によると考えていい．一方，運転者の誤りで事故を起こし，歩行者や他の第三者を巻き込む事故に契約はあり得ない．このような場合，リスクを低減するというよ

りも，当該事故を目（センサ）で直接検知して，確実に（確率に頼らない方法で）危険を回避するという制御の課題となることは明らかである．

自動車の安全は，明らかに制御の課題であるが，一般に制御工学で扱うような原因を操作して目的の結果を得るという合目的的制御ではない．安全の制御は，事故を未来に定め（予測し），これが起こらないためのプロセスを先んじて実行して起こらなかったという「無事」の結果を得ることであり，間接的には，機械の運転効率を上げるなど積極的効果もあるが，もともと非合目的的制御には，積極的な評価がなされ難い．

目的と成果が直接見え難い反面で，制御の失敗者に対する結果責任を課すのは容易である．事故を防ぐ目的をもって何よりも強く要求されるべき自動車の安全制御だが，鉄道やエレベータなど他の機械の安全制御とは異なる扱いがなされてきた．機械安全では致命的被害の発生を許容しないが，自動車の場合，数千件の死亡事故が毎年繰り返されており，人の責任に委ねて，死亡事故を社会的に受容しようとする姿勢が見られなくはない．そしてその時，「自分には起こらない」という思いでもって，確率的な受容が共有される

３－６　不安のカテゴリー

自動車のように不確実性の高い状態において，人間が機械を操作する状況を想定し，これに安全の原理を適用して考えれば，自動車の安全には従来の機械とは根本的に異なる不安（曖昧性）が多様に存在し，それにも拘らず，事故回避を人間の注意操作に押し付けてきた実態が明らかになる．

自動車社会のシステム（制度，交通環境）として整備される安全，そして，メーカーによって提供される安全な自動車であるが，事故防止の主役はあくまでもコントロールの主体である運転者であり，現実には，運転は不安で一杯である．しかし，不安を「リスク」として心理学的問題として処理されてはならない．不安は，異なるカテゴリーで分類され，異なるカテゴリーには異なる特性があり，したがってその解消の方法も異なる．

結論を急げば，機械の安全に伴う不確実性（不安）が，事前策で残留する第 1 の不安（評価は“リスク”），制御の失敗による第 2 の不安（訓練，資格，高信頼性：評価は“信頼性”），事故回避のバックアップで残る第 3 の不安（安全装置のフェールセーフ特性：評価は“非対称誤り率”），最後に事故の責任における第 4 の不安（保険，コンプライアンス：評価は“補償”）という評価と対応の異なる４つの不安のカテゴリーに分けられる．

図 3-2 は，カテゴリーの異なる「不安」を，それぞれ，①リスクベース（リスク），②制御ベース（失敗確率），③フェールセーフ（非対称故障率），④補償（保険の条件）とし，残留リスクで最初に生じた「不安」の解消をそれぞれの立場から丁寧に行って，最後に被害の救済を保険が引き受けることの確証を得て，やっと真の「安心」に達するとする，不安解消のプロセスが存在するということを示している．

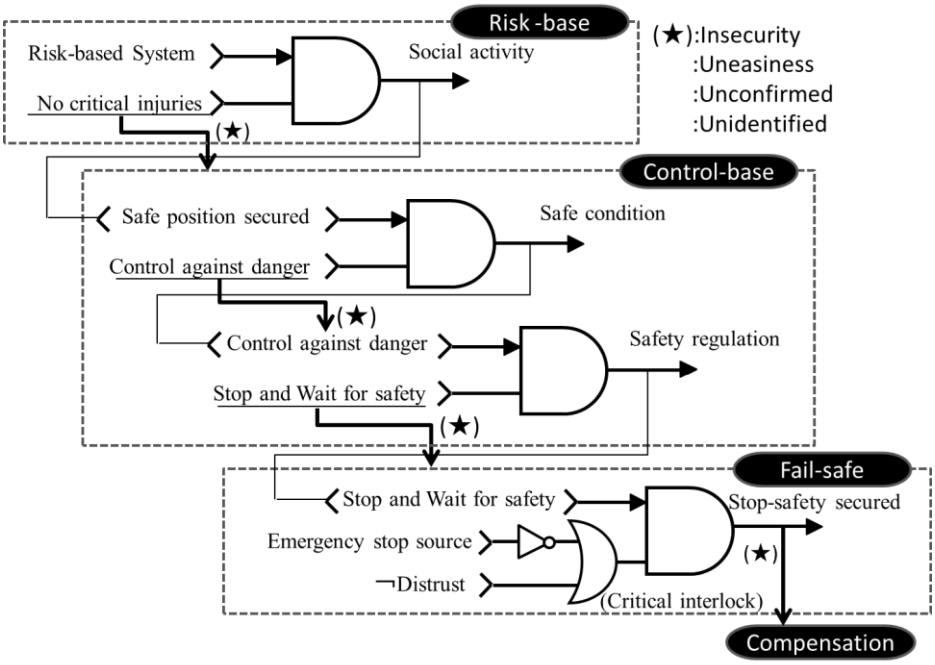


Fig3-2 不安の階層とクリティカルインターロック

リスクは，解消を求める不安の明確化と見ることができる．許容リスクレベルに許容し難い事故の可能性が含まれる場合の不安に応えるのが，制御の安全（運転）である．自動車事故には許容リスクで割り切れない事故が含まれ，その可能性がある限り不安が生じ，自動車の運転には安全のための独自の制御の構造があり得る．しかし，人間特性や技能に依存する限り，例えば，ハンドル操作やブレーキが遅れて追突するなどの不安は解消されない．そこで，その不安解消に有効な工学手段が，後で論ずるように機能安全を採用したバックアップ手段である．例えば，運転者が見失った障害物を検知して自動的にブレーキ操作がなされる．しかし，この装置も故障した場合の不安が残る．故障しない機械はないし，完全なフェールセーフもあり得ないからである．残る不安はわずかだが，完全というわけではない．残る不安を消すのは，救済としての保険である．そして，不慮の事故として保険が引き受けてくれるか否かが最後の不安である．すべての不安のカテゴリーをクリアすれば，このように，安全は安心を得て，絶対安全はないが，安心できる安全はあり得るという結論が期待できるのではないか.

３－７　制御による安全

制御による事故防止には安全（確認）の原理（杉本，蓬原，1990）「危険の可能性のある機械的操作は安全確認を条件とする」が存在し，危険な時は勿論のこと，安全が確認できない（不安）とき，操作を禁止することで確定論としての安全の基礎が与えられる．つまり，不安の時は停止すること，少なくとも事故の対象の手前で停止することである．逆に，事故は，停止が間に合わずに起こるところの事故の対象との接触に他ならない.

事故の回避の典型を人が自動車を運転する状況で考えてみる．人が自動車を運転するとき，前方に安全を確認すると，その状態を積極的に維持しようとする．これが「安全」の判断に基づく安全維持制御（図 3-2 の Safe position secured）である．また，前方に危険（事故の対象）を認めると，ハンドルで回避する，あるいはブレーキで速度を下げるなどによって，危険の空間的／時間的回避操作を実行する．これが「危険」の判断による危険回避(Control against danger)である．そして，さらに危険（事故の対象）に接近したために回避が間に合わないとき，危険の手前で停車させて危険が去るのを待ち，安全が確認されると運転を再開する．これが，「不安」の判断による待機(Stop and wait for safety)である．ここで重要なことは，危険（事故）の手前で「待つ」という制御結果には誤りが許されないことである．他の制御の誤りは安全上許されるが，事故の手前での停止には誤りが絶対に許されない条件で，「待機」が実行される．

しかし，現実には，人間の停止操作には遅れる側の誤りが避けられない．自動車の運転には，本質的にこの特性による不安が残る．そこで，停止操作が間に合わなければ，強引に割り込んで，強制的／受動的に停止させる手段（ブレーキ遅れに対するフェールセーフ・インタロックによるバックアップ）が必要となる．

機械安全では，フェールセーフ・インタロックは，常識的に採用すべき安全手段である．鉄道では，運転士の停止の遅れを補完するために ATS が導入される．自動車では，従来技術で実現できないために不安な運転に人間が右往左往しているのである．

３－８　小括

前述したように，前方に事故の対象を認めるとき，人間の運転には，「安全」，「危険」，「不安」という 3 つの運転モードがある．それぞれ，安全維持制御，回避制御，待機である．制御の危険な誤りは，結局，「待機」における正確な停止操作に委ねられる．しかし，人間の能動的な停止操作には明らかに遅れる側の誤り（危険側誤り）が含まれ，自分の停止操作の遅れを自らによる緊急ブレーキ操作では対処できない．このときの「不安」は，遅滞なく停止する装置に頼る以外にはできない．この危険側の誤りを防ぐためにインタロックを構成する場合，ブレーキの遅れを検知してインタロックで自動的に（受動的停止制御）ブレーキを作動するという方法は採用できない．停止の遅れを検知しても，すでに危険な状態になっているからである．

「不安」の判断で停止操作を確実に行うことが決定的に重要だが，結局，停止の決断が遅れて間に合わず，事故になるのである．一般に機械安全は，制御をコンピュータに任せ，「不安」→「停止」を確実に行うため，安全確認型のインタロックを採用する．自動車においても，誤りを許す判断・操作を人間に委ね，事故の対象の手前の決まった位置で停止操作が完了していない場合は，受動停止操作が実行されるというインタロックが導入されるべきである．運転を人間に委ねる限り，このようなバックアップが必至だということで

ある．

制御において，不安を解消し安心に至るプロセスを不安のカテゴリーとして示し，不確実な中の運転に伴い増大する不安を解消へと導くための構成について述べた．安全条件が明確でないから人に任せ，経験的に安全条件を身に着ける（人間を学習機械として安全（危険）を学習させる）のではなく，不安を解消していくとは安全条件を明確にしていき，明確にされた中でこそ実行できるという構成である．

ここでは，危険な操作に安全の原理を適用し，機械の安全に伴う不確実性（不安）が，事前策に残留する不安（評価は“リスク”），制御の失敗による不安（訓練，高信頼性：評価は“信頼性”），バックアップで残る不安（安全装置のフェールセーフ特性：評価は“非対称誤り率”），最後に事故の責任における不安（保険：評価は“補償”）というように，評価と解消方法が異なる 4 つの不安のカテゴリーに分けられること，そして，初めにリスクとして生じた「不安」の解消をそれぞれの立場から丁寧に行って，最後の救済を保険が引き受けることの確証を得て「安心」に到達するとする不安解消のプロセスを示し，特に制御における不安解消のプロセスについて検討を行った．

第 4 章　防御構造の構築

４－１　基本コンセプト

私たちが信頼性というとき，異常となる事象を捉えて評価する．しかしそれが正常な時を考えると，それは一般に耐えている状態と言える．様々な作用力に対し耐えているから保たれている．ここでは多くは受動的能力であり，環境に対し即応的な能力として耐えていると言える．しかし能力には限界がある．この限界を超える作用力が受動的能力を超えて異常事象を生じていると言える．一般に，この限界を前提におきながらも，作用力と受動的能力を確率分布化し，限界を確率的に扱ったのが信頼性（例えば図 4-1 ストレス-ストレングス モデル）である．しかし安全はこの限界を認識し，これを超えないということを明確にすることである．

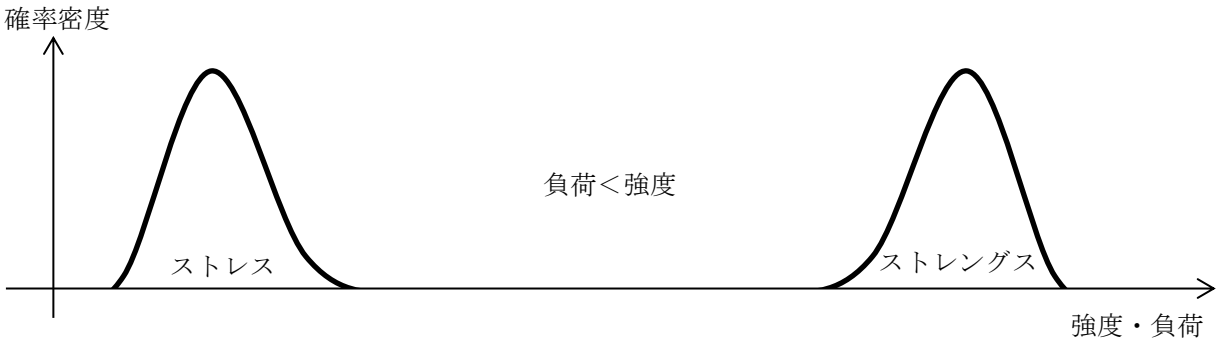


Fig.4-1 ストレス - ストレングス モデルの概念

また，私たちが，リスクと言うとき，防ぐことをあきらめているわけではない．予測をし“回避する”という行為を取り，それは能動的能力と言える．そしてこの能力にも限界はある．

「能力には限界がある」この理解が必要である．物理的能力は限界を理解しやすい，しかし認識能力の限界は理解しづらい．能力とは可能性に対する制御性である．その限界を見極めるとは能力が制御可能な境界を定めるということである．圧力容器で考えてみると，圧力とは容器と気体(液体)の作用反作用として生じている．つまり，圧力制御は耐圧容器があるから可能ということであるが，その相互性が成立する範囲（限界）において扱うことが可能となる．

私たちは境界があるから制御しているように感じる．圧力容器の許容圧力があるから使用圧力はそこから離れたところで制御されているという感覚であり，きちんと制御されればそれを超えることはないという感覚である．それはただ単に設定しただけの境界である．そのような境界であればどんなものでも設定可である．

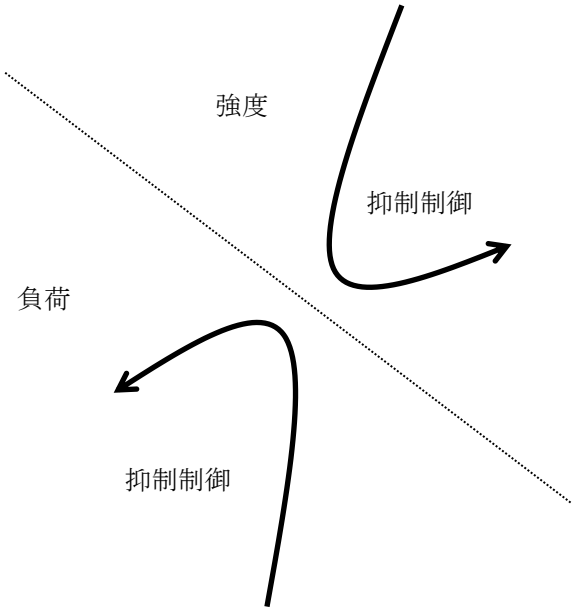


Fig.4-2 ストレス - ストレングスの制御概念

境界とは制御によって明確になってくるものである．圧力容器の場合，ストレス・ストレングス・モデルがあるが，それは圧力制御と耐圧制御(一般的には劣化設計・メンテナンス)のそれぞれが存在しないことにはその境は明確にならない（図 4-2)．

これは，圧力制御は耐圧制御により保たれている耐圧の中でこそ可能であり，また耐圧制御も圧力制御により圧力が制限されるからこそ耐圧の保持が可能であるという相互性がある．

耐圧＞圧力，この関係がその存在の確からしさの相互性である．またこの相互性は事故となる相互性でもあり，否定（圧力＞耐圧）により表される相互性である．境界が生じるとは事故とならない相互性を確かにすることであり，境界を境にしてその相互性の現れ方が変わってくる．能力に限界を与えるのはこの相互性である．限界とはこれ以上は出力できない等の能力を持たないという限界ではなく，その存在を否定される限界である．自身を規定するのは，自身を否定するものであり，相互性の矛盾により否定される．そして自身を規定するその限界が能力に制限を与える．その限界に対して，制約的な規制が生じる．この点については 5 章において調整制御として詳しく述べる．

改めて，分けるという行為により境界が生じる．この境界の明確さは，分けるという行為の明確さによって現れてくる．制御の場合，通常，目標値を持ちその目標値への到達のための調整を行っている．しかしこの場合，境界を超えることに対し「そうならないように」という制御である．

この相互性において離れている（隔離的である）を維持するのが，安全制御であり，そこにできる状態が安全状態である．

これは，次のように表現でき，

防護能力　≧　危険エネルギー

この関係が本質安全であるといえる．そしてこのような関係を防御，このような制御を本質安全制御と呼ぶことにする．相互的な制御による隔離構築とは，

防護能力（劣化防止制御）　≧　境界　≧　危険エネルギー（エネルギー抑制制御）

としての境が明確になってくることである．このような境界生成こそ隔離である．

一般に最大許容圧力を定め，材料はその値よりも劣化しないように，圧力制御はその値を超えないようにやっているように思われる．例えば，リスク・パラメーターには「危害のひどさ」「発生確率」などあるが，ISO26262 においては制御可能性が加わり，またプラント・メンテナンス等においては損傷等の検知可能性がある．これらが単に信頼性なのか，それとも確認可能な形で作られているのかで，その評価は違うはずである．それは境界概念（図 4-3）を明確に作ることになるかならないかの違いである．

これまで防護手段として圧力容器の材料強度と，安全弁や圧力制御系の両面から事故を防ぐアプローチがなされてきたが，有機的連係がなされてきたとはいえないと考えている．そこで，本章では，材料安全(防護)と機能安全(本質安全制御，インタロック)が融合した安全防御システムの構築を検討する．本章では圧力容器技術を対象とした印象が出てしまうが，これまで別々に扱われてきた材料安全と機能（制御）安全の役割と関係性を明確にし，両者を融合することにおける例示的なものであり，一般化された安全確認システムへと繋げる足掛かりとしてのイメージである．

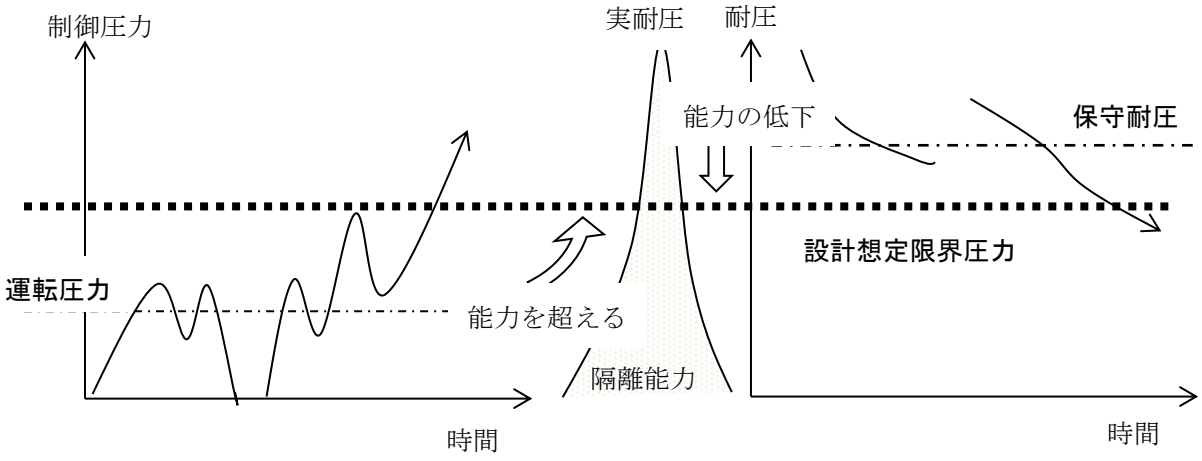


Fig.4-3 運転とメンテナンスの境界概念

４－２　安全確保のための防御

以下，特に断りがなければ，圧力容器についての言及である．人間が高圧に暴露される危険状態は，圧力容器の破裂によるものであり，そのまま危害発生を意味する．安全の基

本原則を定めた ISO/IEC-Guide51 によると，通常，リスク（危害のひどさ×発生確率）は，危険状態に伴う被害を予測・評価するものである．一般に，危険状態が直ちに危害へとつながるわけではないが，安全は，危害の回避を期待してリスクの低減を求めているといえる．

圧力装置の安全を考える場合，危険状態を防ぐ制御（防御:Defense for security）をどのように実行するか，安全の構成論理を明らかにする必要がある．すでに述べたように，圧力容器は破壊（圧力）に対する防護（Protection）のための手段である．しかし，防護の能力には限界がある．問題は，防御手段の能力は無制限というわけではなく，使用を誤って破裂を生じ得ることによる．

防護能力（耐圧）はしきい値特性を持ち，能力を超えた内圧によって破裂を生じる．防護能力を規定することは防御能力の限界が規定されることでもある．そのため能力を超えない（つまり，その限界の中に抑える）目的で内圧を制御する必要がある．当該制御をここでは本質安全制御と呼ぶ．（図 4-4）

ここでいう防御とは，防護手段の防護能力を用いて危険状態の発生を阻止するため，危険源の条件を防護能力内に抑えるための操作（本質安全制御）を伴う，積極的防護を意味する．

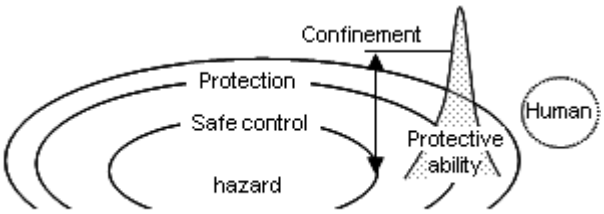


Fig.4-4 防御システム（自己インターロック）概念

４－３　危険空間と安全の条件

ISO/IEC-Guide51（ISO，1999）や ISO 12100-1（ISO，2003）に見られる危害発生のプロセスによれば，危険状態は「人間が危険源に曝された状態」であり，危険状態においてリスクとして評価される．

安全システムの構築は，危険状態になることを阻止する防御（Defense for Security）が基本であり，防御の破れが安全側へと収束できないとき危険状態となり，この危険状態における防御の遅れがリスクとなる．そのことから，検討するシステムは危険状態を阻止してリスク発生を防ぐという防御の考え方で安全システムを人間機械系で再検討する．

まず，安全の論理的関係を人間機械系によって考察する．図 4-5 は，人間と機械の安全（作業）空間の関係を示している．

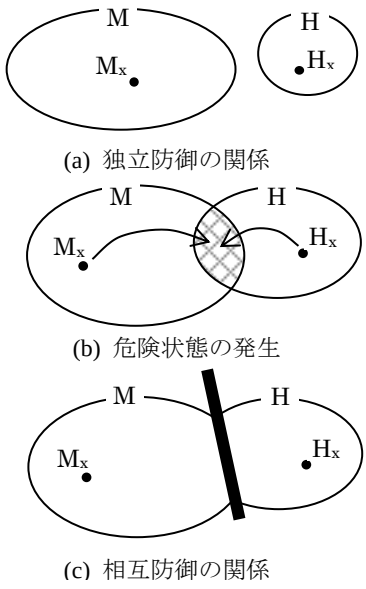


Fig.4-5　安全・防御空間

同図(a)は，人間と機械が相互に独立した安全空間（M:機械，H:人間）を持つ場合であり，それぞれ誤って相手の安全空間に侵入しない条件で，機械安全は確保される．

危険状態は作業空間の重なりにより発生する．同図(b)は，危険状態の発生を示し，原因は，人間が誤って機械の空間 M に侵入する場合，又はその逆の場合，又はその両方の場合に，共有空間で生ずる．危険状態（共有空間）の発生（M∧H＝１）を防ぐには，それぞれの安全空間が，相手の侵入を防御しなければならない．この防御は相互独立の関係にあり，防御すべき人間の安全空間は人が危害を受けない空間であり，また機械の安全空間は機械が危害を与えない空間で，これには，機械の運転が確保される空間を含む．危険状態が即時危害となる場合，相手の侵入の検出を待って対処するのでは間に合わず，危害を防ぐことはできない．事故を確実に防ぐには，共有空間での M∧H＝０を確保するためには，￢M=1 且つ￢H=1 としなければならない．すなわち，機械の安全空間への人間の侵入に対する防御，及び人間の安全空間への機械の侵入に対する防御という，独立した 2 つの防御が必要だということである．ただし，人間に安全の防御は期待できないから，後者の防御は，自ら機械の安全空間を逸脱しないための自己防御的形態となることが示唆される．ここでは，「防護」より積極的である「防御 defense for security」を用いている．

図 4-6 は安全確認システムであり，図 4-5（a）を「隔離の安全」として確認し，安全を確認できないとき「停止の安全」として停止する．

Fig.4-6　安全確認システム

４－４　危険状態の発生に対する防御

危険状態を阻止するには，危険源 M と人間 H をそれぞれの安全空間に隔離し，互いに相手の侵入を阻止する積極的防御が必要である（図 4-5(c)）．危険源を圧力とすると，圧力の拡大(破裂)の防御手段が圧力容器であり，その内部が安全空間である．破裂は，周辺の人間に及ぶので，圧力容器の防御は図 4-5(c)を修正して図 4-7 のように表せる．

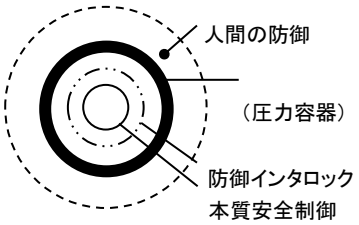


Fig.4-7　圧力容器の防御の構成

この防御能力は，作用／反作用の受動特性，ここでは，内圧に対する遅滞ない反力の発生という弾性材料の特性に依拠するものであり，もし圧力検知に応じて防御のための力を能動的に調整するという，いわゆる「制御」では遅れによる危険状態の発生は避けられない．そして，圧力容器は必然的に防御能力の限界が，材料の特性(弾性限界)や構造によって生ずる．

圧力の側から危険状態が生ずる場合，

・防御能力（材料の弾性限界で定まる）＞破壊力

人間の側から危険状態を生ずる場合，

・防御能力（人間に対する security）＞破壊力

によって危険状態が防御される．ただし，人間の侵入に対する防御は，物理的防御(柵や囲い等)だけでなく仕組み（キーシステム等）による防御が構築される．ここでは，前者の防御を考える．

一般に，防御能力とは，機械系では例えば車輪の脱線を阻止する機械的力であり，化学系では爆発温度，電気系では耐電圧，圧力容器では弾性強度と構造で決まる耐圧であろう．

４－５　防御能力における制御

４－５－１　防御と本質安全制御

例えば，爆発性ガスは，爆発温度に達するまでは，爆発が阻止されている．爆発温度がしきい値となって防御限界，すなわち防御能力を与える．圧力容器は，破壊圧力（しきい値）に達すると破裂するが，破壊圧力までの防御能力を有すると解される．

このことは，危険源の安全空間外への逸脱を防御するための手段には能力に限りがあることである．そのため，危険源が防御能力を超えないための積極的操作が必要であり，この操作を本質安全制御と呼ぶことにする．

一般に，機械は，本来の目的を実現するための制御を実行する．これは一般に危険源の能力の有効な使用に基づく．つまり危険源は，本来は仕事のためのエネルギー（資源）である．しかしその一面で，破壊の能力を持つ．つまり目的を誤ると，防御の限界を超えて危険状態を生じうる．防御の限界を超えた危険状態において破壊を生じ危害へとつながる．

つまり，本来的制御と並行して，場合によっては優先的に，本質安全制御，すなわち，危険源が防御能力の限界を超えない目的で行う制御を実行するのは必須である．この制御の必要は，本来的制御には，誤って防御能力を超える操作の可能性があるが，その誤りは許されないという現実的制約に基づく．

例えば，車で目的地に向かう場合，運転操作には，安全(運転者の防御能力：左車線であり車線内であることを守る等)を維持する操作が含まれ，むしろ優先される．疲労で車線内を維持できないようなときは，目的以前に運転は禁止される．目的に向かうことに事故が含まれるのではなく，車線を越えることが事故へとつながる．

また，圧力容器は，目的の圧力を制御するが，誤りがあっても少なくとも防御能力を無視することがないような操作が行われていると考えてよい．目的圧力への制御を高信頼性で行うのではなく，目的制御とは別に，目的制御に優先する防御能力を超えないという制御が行われると考えるべきである．

４－５－２　防御とその限界

防御は防護と本質安全制御で構成される．繰り返すが，防護能力には限界があり，この限界を超えた使用がなされてはならない．この限界を超えない制御が本質安全制御であり，その制御の失敗で限界を超える場合は，運転を停止させる．これがフェールセーフインターロックである．

しかし，寿命・劣化等により規定された防護能力が低下し，フェールセーフインターロックで安全と判断する基準より低下する場合が起こる．防護能力の低下は疲労やき裂などの経時的劣化に影響を受ける．この劣化特性が認識できれば，使用時間（回数）を限定することが可能である（時間的インターロック）．メンテナンスは防護能力の限界が劣化するのを監視しているといえる．防護能力が制御能力との間で作る境界まで劣化（能力低下）する前に補修・交換をし，限界に達する前に停止（大規模改修や廃棄）させる．

例えば，材料の損傷において，目視での検査としている場合，それは表面への目視可能な（例えば 1 ㎜以上の）傷がどこまで増えたら装置を破棄（停止）しなければいけないかという制約がある．傷の数が連続的に増えていってある X 個以上になったら，また傷の大きさが連続的に拡大しある Y ㎜以上になったら，許容範囲の逸脱であり使用停止というよ

うに設計されているからこそ可能なメンテナンスである．もしこれが隠される，また，場合によっては様々ということになれば，経験・勘・確率によるとなってしまう．目視検査の場合は目視可能な構造であるからこそ確認構造を取ることができ，また，繰り返し確認すること（独立的なら）で見逃す可能性を減らしていくことができる．そして制限に対し停止（廃棄等）というインターロックをかけることができる．

この場合でも，疲労・劣化等，経時変化は，使用条件で変化するため，正確に使用時間の限界が判断できないかもしれない．しかし安全率による延命処理は正確な寿命の判断より，寿命を大きく遠ざけることで，寿命と廃棄基準年数との交差がないと期待するものである．寿命限界の問題は，今後の問題としたい．

しかし，日本においては作ったものをうまく検査するとなるが，本来であれば検査可能なものを作るとならないと，特にその被害が容易に受け入れられないものについては，安全を確保するとは言えない．目視だけでなく音響・超音波や磁粉探傷等様々あるが，“作られたもの”に対し様々な手段を適用してみて“見つける”のではなく，損傷発生プロセスを「まだ許容範囲である」と確認できる構造が必要になる．

また，メンテナンスも事故を防ぐという明確さがなく，曖昧なまま行うということは，経営にとっての削減対象と容易になりうる．法令で決まっているということしか，その根拠がないことになり，逆に法令で明確でないものは削減されてしまう．

ところで，安全確認システム（自己インタロック）における安全確認とは，危険源のポテンシャル（破壊力）が防御能力の限界の内にあることの確認であり，本質安全制御に対する正常確認を意味する．そして限界内にあるという確認のための監視ポイントが要求される．この防御の限界は，防護の限界と制御の限界から定まる．防御の限界は，制御の限界による遅れが防護の限界を超えないことを保証するしきい値であり，防御による回復性を保証できる最終帰還点（point-of-safe-return）である．材料においては，たとえば降伏点であり，危険エネルギーに対する応答能力の限界（弾性限度）が明確に示される．そのため，危険エネルギーを能力の中（弾性域）に抑える制御が入る．しかし制御には遅れが生じる．制御の応答性により弾性域＝回復性を保証する限界監視点が設定される．

４－６　インターロック

４－６－１　インターロックシステム

さて，防御能力内に危険源のポテンシャルを抑える操作（本質安全制御）であるが，この操作にも誤りが含まれると考えなければならない．特にこの場合の危険側誤りは防御能力を超えるような圧力上昇挙動を含むので，本質安全制御に対する結果の正常確認，すなわち安全確認を行って，これが確認できない場合並びに規定圧を超える圧力上昇挙動を示した場合には，圧力上昇の操作を停止させる操作（防御インターロック）が行われる．

現実には，電源を遮断して，加圧手段の運転を確実に停止させる．この場合，圧力の安全確認のためのセンサは故障のとき「安全」の通報をしないフェールセーフな特性を持たなければならない．

このように，安全確認とは，防御能力に限界があって，危険源のポテンシャル(破壊力)が防御能力の内にあることの確認であり，本質安全制御に対する正常確認を意味する．

序章の図 1-1 は，圧力容器の防御能力の限界のために，これをさらに防御する関係で防御層が構成されるシステム防御を表している．情報的防御，機能的防御，物理的防御を階層化し，安全防御システムを構築することができる．

これまで，安全確認システムは，作業空間に人がいないこと(安全)を確認して機械の運転を許可するインターロックに限定された．しかし，本論では，危険状態の発生理由を，人間の侵入だけでなく，機械（危険源）の人間空間への逸脱を含めて一般化するものである．機械的ガード，圧力容器等にとって，物理的防御が人間と機械（危険源）を確実に隔離するが，「防御」という積極的危険状態回避を導入することで，より一般性の高い安全確認インターロックシステムが導出できる．

４－６－２　空間・時間のインターロック

災害を防止するには，これまで述べたように「隔離の安全」「停止の安全」により危険状態を作らないことである．ここで考えなければいけないのは図 4-5（b）において，作業空間接触時には停止が完了していることが要求され，停止には遅れが許されない．遅れにより危険状態（重なり）が発生する．

まず隔離の安全として，人間－機械系が空間としての分離を行い，離れていることの確認に基づくインターロックが構成されていると見なしうる．

また，機械と人間の接触が不可避な場合，接触前には停止は完了していなければならない．しかし停止に時間がかかる現実的制約から停止時間の条件が存在する．接触後短時間で停止すれば危害を生じない場合もあるが，厳密には，危険状態が発生する．これにより作業空間接触と（接触前の）停止の時間的逆転からリスクが生じる．

このときにおいて確認とは，この「停止にかかる時間条件」より離れていることの確認であり，接触前に止まれるという確信的な確認であるからこそ安全確認である．この条件を満たさない場合は危険監視・検出である．危険を検出してから対応するのではその対処がうまくいくことに保証はない．監視するとは「止まれる条件を確保した領域」の外を監視することであり，その中において危険が発生しない構造が要求される．たとえば圧力容器でどの圧力でも破壊の可能性があるとなると許容圧力の設定もその監視も意味を持たなくなる．

停止にかかる空間を除いたとき，その残りの空間においてどれだけの余裕時間があるかで確認サイクル時間が変わってくる．そのサイクル間においては速度を一定と保証するか

最大速度を保証するかで変わるが，そこにおいて生じる時間が次の確認までの時間でもあり，また自由に使える時間でもある．しかし，その時間の遅れは許されない．それゆえ遅れ側は許されない時間のインターロックが入る．また時間的に区切ることで確認の多重化を行うことができる．

４－６－３　相互・自己インターロック

さて，接触直後に停止により危害を回避する場合の人間・機械の共存は，停止時間をできるだけ短くすることでリスク低減を図る．しかし，人間が容易に接近可能な場合，たびたび停止しては仕事にならないし，またリスクが発現した時は再稼働の保証も覚束ない．

従来の“安全確認システム”は，本来このような生産効率上の問題を含んでいるにもかかわらず，それが指摘されないのは，安全確認システムには，「安全」を積極的に作り出し，停止を回避するシステムが組み合わされて効果を発揮してきたからだといえる．仕事において，相互に隔離された状態が「安全」であり，人間は機械の領域に侵入しない，また，機械は人間の領域に侵入しない意識的操作によって，機械の稼働率が維持されてきたといえる．機械が人間の領域に出ないという操作は，現実的やり方として，機械の安全の条件を規定して，その条件を逸脱しないための操作を実行するという自己インターロックが構成される．

安全確認システムは，作業空間に人がいないこと（安全）を確認して機械の運転を許可する．危険状態を生成させない条件では，相互に“相手を入れない制御”が要求される相互インターロック構成である．しかし危険状態の阻止を，人間の侵入だけでなく，機械（危険源）の作業空間からの逸脱（人間空間への侵入）を含めて一般化する必要がある．この様に，機械には“出ない／入れない制御”が要求される．このいわゆる両立性（Compatibility）を達成（図 4-5（c））する代表的なものが構造材料による防護である．圧力容器による防護で述べたように，材料安全の特性，すなわち，「押されたら，即押し返す」という能動性（作用／反作用）には遅れの概念がない理想的防御手段と見なすことができる．機械的ガード，圧力容器等による防護は遅れのない理想的防御手段であるとはいえ，隔離の能力に限界があり，その能力の限界に対し，他の防御手段で積極的に補うことで，階層的防御システムが構成され，より一般性の高い自己インターロックシステムが導出できる．

４－６－４　安全における寿命

一般に製品は，防御の能力により積極的に保持されているともいえる．そして能力からの逸脱において危険状態が発生している．ある意味，危険状態の発生が製品の死といえる．そして防御におけるインターロックの破れが寿命である．インターロックが機能している間は，部品交換され，又は機能性が落ちれば廃棄される．いわゆる価値・機能・物理寿命

である．インターロックの故障は安全寿命ともいえる．安全側故障は修理されるため，製品を長く使うと，インターロックの危険側故障で終わることになる．

４－７　防御の階層

先に「隔離の安全」と「停止の安全」による安全を挙げたが，隔離による安全の積極性は人を守るだけでなく仕事を守っている．停止による安全は，危険状態の発生に直面し，人を守るために仕事をやめる（機械を止める）選択である．人も機械も目的は仕事にある．危険状態で止める前に，止まらない（危険状態にならない）ように積極的に隔離状態の維持を行わなければならない．このため人を守る防御の上に，仕事を守るための防御を必要とする．防御は守るべき目的で階層化される．人を守るから，その上に仕事を守るシステムが構築できるのであり，その逆は社会的に容認されないであろう．傷害事故等は仕事自体の禁止ともなる．もし仕事を守るのなら，それに先立って人を守る必要がある．

防御能力を超えたときに次なる均衡点へ導かれる．この均衡点が崩れないように防御が行われ，この防御の中で目的への復帰処理が行われる．防御は目的からの逸脱を回復させることで階層化される．

実際的には，危険エネルギーが能力を超えていくことに対し，防御において２つのタイプの階層が構築される．一つは自己性に対してであり，もう一つは相互性に対してである．

自己性においては，防御の能力を規定し，その中に抑える制御に対し階層を構築していく．危険源に対して防御が行われ，防護能力に対し，制御能力で階層が形成される．

それは新たな階層を内に外にと作っていくことになる．防御が破れた場合，防御の能力を超えたエネルギーを新たな危険源として，新たに防御が形成される．この過程でエネルギーを吸収・拡散などで低下させる構成をとることになる．これが外に作られる階層であるが，逆にこれにより内の階層はその規定が明確になってくる．危険源を明確に捉え，そのエネルギー変換の流れの方向に対し階層が作られる．

しかしこれが許容されるのは自らのシステムとしての範囲を逸脱しないときであり，システム内階層としての自己性である．そしてシステム外部に対しては，相互性としてとしての階層が構築される．これは社会による防御階層ともいえる．個人（企業）システムからの逸脱は，他の個人や社会としてその被害を受けるままに放置するわけにもいかず，また禁止としても実行前ならともかく事故の進展に対しその強制力（消防等）がないと禁止はできない．自己性の階層は自らによる許可／禁止の階層といえ，相互性の階層は社会との関係での許可／禁止の階層と言える．

防御の階層は，内側の能力を超える（危険エネルギーと防御能力の関係性）ことに対して作られ（安全設計），外側の能力（防御能力の限界と逸脱エネルギーとしての依存性）に入れることによって評価される（リスク評価）．この関係性のゆえに，防御階層には事故が歯止めなく進展していくような共通原因故障等のない独立性が求められる．

４－８　安全コンセプト

防御能力により安全関連部を考え，防御能力の限界を超えることを危険側故障としてモデル化している．圧力容器等においても物理的防護層としての明確な制限の役割が求められる．そして内圧に対し圧力容器が提供する遅れのない応答（制御）を維持するため，防護層の能力を超えないための制御階層が構築される．能力の限界（耐圧）という明確な指標の中で，その圧力の積極的なコントロールで防御が行われていく．

事故は危険状態の発生から起り，危険状態は防御能力の限界で起る．防御の限界を超えるのは，制御の失敗または防護の欠陥においてである．この失敗・欠陥を回避するため，一般に冗長系・多重・多様系といった組み方で構成しているが，確認という構造は明確ではない．それゆえ何が制限なのか，それを明確にした制御が行われていないと考える．

制御において，フェールセーフは防御としての OFF 能力であるが，信号としてのゼロでなくエネルギーとしてのゼロ，つまりエネルギーの消散完了を意味する．そしてその多重化等は防御のための維持能力である．事故の前に止めるとは，危険源のエネルギーと防御能力が逆転する危険側に対し，防御能力の上限に対して遅れのないリミッターが安全防御システムの課題として明確に示され，超えない確実さとは，回避や抑制でなく停止の確実さである．

４－９　小括

本章では次のような検討を行った．

（1）人間と機械（危険源）が危険状態を生成するが，危険状態の発生を阻止する防御の考え方でより一般化された安全確認システムの提案を行った

（2）防御能力の限界を超えないための制御(本質安全制御)の必要性と，その理由を示した

（3）危険源のポテンシャルと防御能力との関係で定まる安全（security）を，圧力容器を通して考察した

（4）防御（security）が，本質安全制御とインターロックによる多層の防御層を形成することを示した

なお，防御能力は，故障，人のミス，寿命，使用環境で低下を加速するが，そのインターロックへの影響は今後の課題である．

たとえば圧力装置のような一般に高リスクとみられる製品においても，それを普及させるのなら，リスクは必ず発現するとし，その危害をユーザの受容レベルへと入れなければならない．それは危害のプロセスにおいてどう介入したかの問題であり，ベネフィットがあれば高リスクも受容されるという問題ではない．「隔離の安全」「停止の安全」など，危険状態が生じない条件を確保するのが製品としては基本である．その基本を踏まえないリ

スク評価は，前回よりも「上がった」・「下がった」として，その前回に根拠はあるのだろうか．一般に「機械は止められない」という声を聞く．もしかしたら「止められない機械」というものがあるのかもしれない，しかしほとんどの機械は止めることができる．本当は「止められる機械」であるのに「止められない機械」として作るということを社会として受け入れていくべきであろうか．

安全な領域は作りそして維持することで，確定的（しきい値）な安全を検討することができる．安全は作ることにより想定通りに実行することであり，想定を逸脱前に止まることであり，維持できないときに止まることである．そのしきい値とは，制御により防護能力を超えないこと，防護能力を低下（劣化）させないことと表すとき，そこに境界を見出すことである．その境界を相互に超えないことで隔離状態が維持される．そして隔離を逸脱する前に止まることでリスクがないと言える．

安全ということを確認して仕事を行うのは，主体的に行う仕事（労働者だけでなく機械においても）にとって必然である．安全構築は，人を守るだけでなく仕事を守ることでもあり，社会に対してもまた仕事に対しても誠実（integrity）な姿勢である．

今回，防護を立て，その能力を超えないための本質安全制御を内に作り出していく防御を基本要素とし，この防御の限界（能力を超える）における依存性により防御の階層を構築している．社会的に受け入れられるとは社会的な防御能力の中に入れることである．ここに展開した防御コンセプトの目的は, ユーザの受容を真の防御層（Independence）とし，そこに依存（Dependence）した防御の概念として安全を構築するためである．

第５章　制御としての安全

５－１　主体としての安全

５－１－１　主体・客体

主観・客観とあるが，主観は制御的であり，客観は確率的（非制御的）である．環境の状態は確率的に表現されうるが，そのレベルでは理解できても，「では自分は」となると何も情報を与えない．それは人間が環境全てをとらえるのはあまりにも複雑すぎるが，確率値で与えられてもあまりにも単純すぎてわからないとなる．確率で均質な状態とされたところに「自分」はない．これは「自分は」という時の階層と合わないと言えばいいかもしれない.「自分は」という認識自体，主観的認識であるが，環境を（限定的かもしれないが）認識し，環境に（限定的かもしれないが）作用しうるという，環境と区分された観念を持つことが主体であることであり，それ故にコントロールしうるという認識を持つといえる．

コントロールしうるとは情報と操作を概念・判断でもって繋げることである．情報とは概念を通した環境認識である．そして，その情報により操作した結果として環境を捉えなおすことで概念化が行われていく．このとき，概念を形成・変更していくことで自身が置かれた環境を理解することになる．

客観的であるとは，主体から独立した視点であり，独立故に非制御的である．直接操作的関与をしえない故に確率的（可能性的）な結果認識を持ちうる．例えば，行政的安全は確率的であるという．それは市民個々人が行政から独立した存在として在るからこそ非制御的であり，状態に働きかける（間接的に）ことになり確率的になる．もし個々人の独立がなく行政に従属的であるならば，行政の直接制御により個々人の安全を達することになる．逆に道具を体の一部のように扱う・感じるとは，この主観的認識の拡大である．道具から機械へと進み，サイバネティックスが身体的拡張と言うとき，この人間の主観性の拡張と考えてもいい．それゆえ人間の安全制御能力を考慮しない人間－機械系は不完全である．

個人にとって安全とは制御的な安全である．そして“安全である”とは，環境に対して明確な区分を見ることである．区分とは構造物であったり社会制度であったりと，物理的非対称性や精神的非対称性として構築されるものが認識されやすいかもしれない．しかし制御することにより区分は生じ，制御され続けることで区分が明確になる．　“自分”と環境を区別する境界を明確にすることは，安全（制御可能）と不安（制御不能）を分けていくことであり，その“安全”を見ている自分がそこに“在る”と確信するからこそ，安全確認により仕事ができる

本論で述べるのは主体としての安全であり，それは制御としての安全である．

５－１－２　信頼像と現実的評価（信頼性）

海保らの「人間工学」によれば，人間には，こうありたいという時の一つの典型として，機械のごとく正確無比に振る舞うことのできる「完璧人間像」がある（海保他，1996）とされる．知・情・意の世界で言えば，例えば，知的活動を完璧に行って，論理学や数学が構築した世界に到達でき(知)，いかなる状況に遭遇しても，感情を最適な状態に保つことができ(情)，意志の力によって，自己を合理的にコントロールできる(意)．しかし現実の人間が，およそ，こうした「完璧人間像」とは程遠いという彼らの主張は当然である．

人間を特徴付ける不完全性と不安定性，そのために生ずる纏まりのない多様性にも拘らず，「人間」としての共通の認識が存在するのは，理想としての完璧人間像を誰もが共有するからではないだろうか．不完全である人間は，「完全」を求める（制御）特性で特徴づけられている．それは「完全」からの差異としてこそ個（自分自身）を認識するがゆえ，と言える．サルトルはポアジュの述べた「人間は人間の未来である」を好んで取り上げるが，「各人がそれぞれ自分自身を選択する…しかしまた，各人はみずからを選ぶことによって全人類を選択する…私を選ぶことによって私は人間を選ぶのである」(J-P. サルトル, 1959)そして，かくあるべき人間像を創って（選択して）いくからこそ，私たちの責任は想像よりも遥かに大きい，と述べる．無目的に生まれた存在であるが故に依るべくない不安があるが，そこにおいて「人間になる」という目的を持つことで私たちは人間として形成されている．ただしそれは機械的な完璧人間像であろうか．

山岸は“信頼の構造（山岸，1998)”において，相手の「能力に対する期待」と「意図に対する期待」とを区別して信頼の要素として挙げている．同様の研究も多く，安全における信頼像について，我々の解釈として，

信頼　＝　目的実行能力　∧　相手への最善の配慮

と考えることができる．「信頼 trust」に関わって，人は相手の期待を裏切る可能性を完全に否定して信頼を得るのであって，裏切る可能性を確率（信頼度）で表して信頼を評価するのは筋違いである．「信頼を求め，信頼に応える」という関係は信頼の完全像が相互に形成される場面であるが，現実には，不慮の結果 accidental event が裏切りとなるような状況が起こりうる．

一般に，不慮による結果が被害を伴う場合に“裏切り”の意識が生ずるのであるが，例えば，被害を最小にする最善の配慮（state of the arts,　best effort principle etc.）を行った結果としての被害を受け入れるというように，信頼関係には「不慮の結果に対する受容の約束」に関わる「事前の合意（事前責任 accountability)」が得られていなければならない．「裏切らない（失敗しない)」ではなく「相手への最善の配慮」という非対称特性であり，この非対称特性が「像 image」として共有される信頼の完全像の真意である．

機械における信頼性などは目的実行能力の確率的評価が行われている．人工物は目的によって形成されるが故に純粋に目的のみ考えているともいえる．単に人工物の扱いを完全に人間によるとしていた時代，使用者が全てを引き受けることができた時代はまだいいが，それは機械ではなく道具と表現できていた時代である．人工物には悪意がないというところに依拠し，設計者は善いものを社会に提供しようとしている，つまり「動機が善なら行為も善」であり，「その結果に責任を問われたら，善いものを社会に提供することができない」という思いを抱く者も多いが，「動機が善なら行為も善」は個人主義であり，「社会への影響に対し最善の配慮」を行うことは社会的存在としての責務である．

「目的における信頼性」が信頼の基本機能ではあるが，そこに「相手への最善の配慮」という非対称特性が入ることで信頼（または信用と述べてもいいが）は完成する．そしてこれは被害を出さないことへのコントロールでありその確実性である．これは目的をしっかりやれば結果的には相手に被害が出ないというものではなく，明確に相手への被害を遮断するために行う制御である．機械でいうと，人間から離れることでもあるが，その確実さとは停止状態であるという確実さである．

５－１－３　制御に基づく安全の要求

私たちは，事故は本来絶対に起こってはならないとする認識と，“絶対安全はあり得ない”とする認識との間の矛盾に困惑する．リスクは社会的契約に関わる指標である．社会が受容する条件でリスク低減が図られるのに対して，事故は個人に生じ，信頼の完全性を裏切る事件（event）である．リスクとは別に，不慮の結果として生じた事故の被害を受け入れ，信頼関係の喪失を防ぐための合意が成立してなければならない．しかし人間は，事故防止の結果が確率論（リスクは大数の法則に基づく）で評価されることを覚悟の上でも，結局は「完璧な安全」に固執している．

安全こそ，信頼の完全像が最も忠実に適用されるべき対象であると言える．そして事故防止ではなく改めて安全確認として捉えられるべき概念である．それは信頼性（事故防止）としてではなく非対称性（安全確認）として捉えられるべき概念である．これは安全を脅かす危険において「危険を検出する」のではなく，「危険がないことを確認する」ことである．先に「隔離の安全」と「停止の安全」という概念があると述べたが，離れている（危険源と主体との分離）という認識でもって安全と認識する．「危険がないこと」とは「危険から離れていること」であり，

① 危険を認識し，そこから離れていると確認する
② 認識の限界を不安（危険）とし，不安がないこと（ある空間を捉える正常性）でもって，改めて危険が“有る”と仮定し，その危険が空間内に「ない」（つまり，離れている）ことを確認する（危険は境界の外から来て，中に突然現れることはない形で定義する必要がある）

この 2 つの確認構造に対し，離れるという制御構造でもって隔離が構成される．これは「危険がない世界」が「安全」ではなく，危険を正しく認識できる主体が離れていると判断することで「安全」とするものである．そしてこの“安全”が常（連続監視）に真であるということ要求するのが「目的を実行する主体（システム)」である．そこでは安全の中に“在る”という制御特性が要求される．

安全とは危険源との分離の完全性と捉えることができる．仕事に必要な危険源を無くすことはできない．故に，仕事をする上では危険源との関係可能性を考慮する必要がある．そして分離の極は関係の完全なる切断であり，可能性を無くすことによる切断である．コントロール可能なのは主体自身であり，その主体が持つ可能性を無くすことである．それが，機械においては人間（危険源）に対峙して停止（一般に固定かつ可能性としての動力の遮断）であり，人間は仕事をやめる（非常停止作動）ことである．やめることで安全が確保できる故に人間は自律的（制御的）に行動できる．しかし単に機械化された作業場は人間がやめても安全が確保されるわけではない．もし人間が非常停止を持たないならば，「やめることはできない」という，人間の自律性を従属させた作業場となる．「やめることができない」とは要するに，人間においては失敗，機械においては故障を許さない作業場ということになる．

この「やめる」という停止特性は自身の特性として決まってくる．そして，相手が「停止特性をとして必要な距離」以上離れていることで，停止は相手には依らない自己インターロック特性となる．確認するとはこの「停止特性をとして必要な距離」が確保されないときは禁止（停止）することである．制御性とはこの“禁止”を非対称性（¬禁止≧制御）として持つことにより自律性として認められる．ここから述べることは，信頼に足る安全な実行とは，

合目的的能力　∧　自己インターロック構造

で示されることになる．

これは，象徴的には，仕事を正しく行わないと安全になると言える．一般に，仕事を正しく行うと安全であるような設計がされるのは当然である．それゆえ信頼性を高めることが求められると言える．しかし，自己インターロック構造とは，安全な仕事であるという正常性が示されないと止まってしまう構造を求めるものである．つまり，安全に目配りしながらも仕事をうまく行うではなく，仕事に集中し信頼性高く行わないと止められてしまうような構成である．

５－２　安全確認の構造

５－２－１　安全確認の原理の論理的関係

安全確認の原理（杉本，蓬原，1990），すなわち「危険の可能性のある機械的操作は安全確認を許可条件とする」は次の論理的不等式で表される．

S≧Se≧Sc(≧P)≧Ex　　･･･(5－1)

ここに，S は安全(真の安全：無事故)を示す 2 値の論理変数である．また，Se， Sc はそれぞれ安全の条件に基づく安全（以降，単に安全条件とする），安全の確認に基づく安全（以降，単に安全確認とする）であり，P は許可，Ex は目的（危険の可能性のある行為）を表し，ともに，2 値の論理変数で表す．さらに，図 5 - 1 に，式(5－1)の安全に関わる空間の構成を示す．

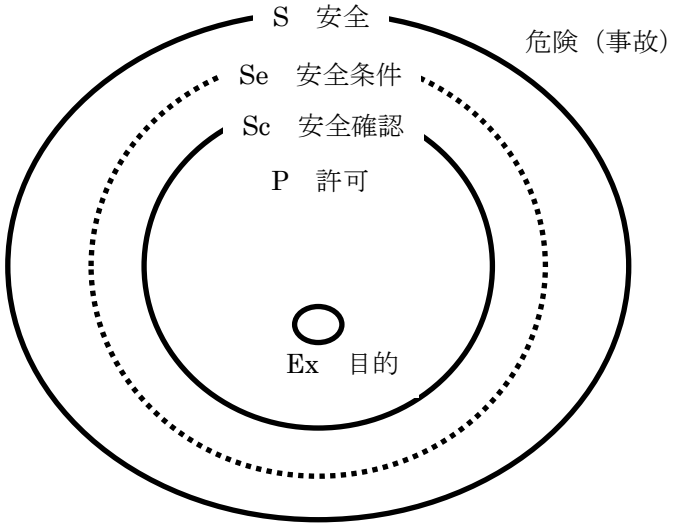


Fig. 5 － 1　安全空間の構造

安全は事故の論理的否定，すなわち，事故の直前までは安全（S=1）である．ここでは安全の否定を危険（H=¬S）とし，事故と同義とする．事故が起こるとしたら必ず危険を経過するからであり，危険を経過しない事故は認識しえない．信頼性ではなく安全性で作るとは，危険の認識構造を作ることである．ところで，危険を回避するための条件としての安全 Se は安全 S の全体を利用できない．直前での危険回避はブレーキでは間に合わない．すなわち，2 つの安全は S≧Se の関係があり，安全 Se には，ブレーキによる不安な空間が除外される．

さて，危険な時（S=0），Ex=1 で事故が起こるから，¬S∧Ex=1 の可能性（確率論的予測を含む）を有するシステムでは Ex=1 は許されない．認証制度によって計画が許可されない場合もあろう．明らかに S=0→Ex=0 は事故防止の絶対条件であり，運行が強く禁止されることを特に Ex≡ 0 で表し，「禁止」と呼ぶことにする．自ら禁止しないとき，この禁止とは自己ではない外部からの禁止として行われる．外部からの強制停止であり，非自律的強制である．車に乗る場合，飲酒時に自ら禁止しえないとき，社会（警察等）から禁止される．このとき運転再開はなかなか出ないであろう．自身ではどうしようもない．大概は飲酒後に自ら禁止することは飲酒故にできない．そうなる前に禁止する正常性がない場合，

それは確認構造のない人間である．安全の中でこそ自律性が認められ，安全の領域を出ることは自律性が否定されることである．安全領域に在ることが正常状態であり，その逸脱とは例外状態であり，そこにおいて決定を下す主権を持つことが否定される．事故が起こるということは，その加害者において明確に主権がはく奪されることであり，国家という（被害者の代理的）主権者が決定権を持ち，制裁が下される．安全領域（正常状態）に対しこの例外状態は不安領域と置いてもいい．そして事故となる明らかな危険を前にして危険領域において異常状態と置くと，自らの主権を意識する場合，それが主張できる正常状態からの逸脱をするわけにはいかない．しかし主権意識のないとき，特に例外状態であっても異常状態であっても，結果として事故がなければ変わりはない．それ故に事故は避けなければいけないと思っても，例外状態・異常状態において回避すればいいとなる．要するに，酒を飲んでいても，見つからなければいい．また，酒を飲んでいても，うまく事故さえ回避できればいいとなる．

安全 S に在ることを確実にする，それが自律性を確保することであり主権を持つことである．安全の中に在ることこそ確認しなければならない．

ところで安全 S=1 は， Se=1 と Se=0 からなる．ブレーキ（停止）が間に合わない条件で目的操作が実行されることは許されない．S=1 で Se=0 の空間は，ブレーキが作動する停止過程ではなく，停止完了であり，Se=0 での停止完了状態としての Ex=0 を単なる停止と区別して「中止」と呼ぶことにする．

Se=0 のときは必ず Ex=0 となる条件で，安全の確認 Sc が準備される．そして，Sc=0 の時は停止して Se=0 による中止を保証するという条件で安全が確認されれば，Sc=1 の結果として許可 P=1 が出力される．このように，誤りを含まない「許可」を得ることが起動時の安全確認のプロセスである．

この実行は

$$Ex = S(Se(Sc \cdot W \vee \neg Sc \cdot Wc) \vee \neg Se \cdot Wb) \vee \neg S \cdot Wa$$

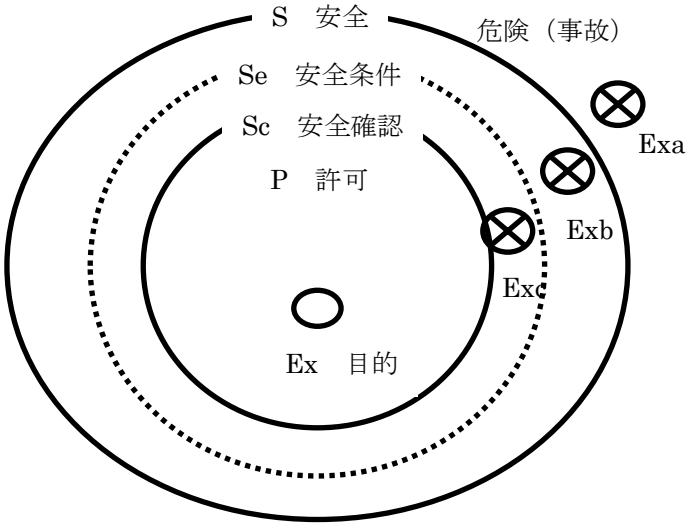


Fig. 5 － 2　安全空間の構造と実行・停止

と表せるが，先の禁止・中止・停止は図 5－2 の Exa=0（禁止）,Exb=0（中止）,Exc=0（停止）つまりそれぞれ式中の Wa=0,Wb=0Wc=0 を求めている．またこのことはシステムを構成するとき，停止というものの確実性を逸脱しない構築，つまり the safe condition としての停止を求める構成である（図 5－3）.

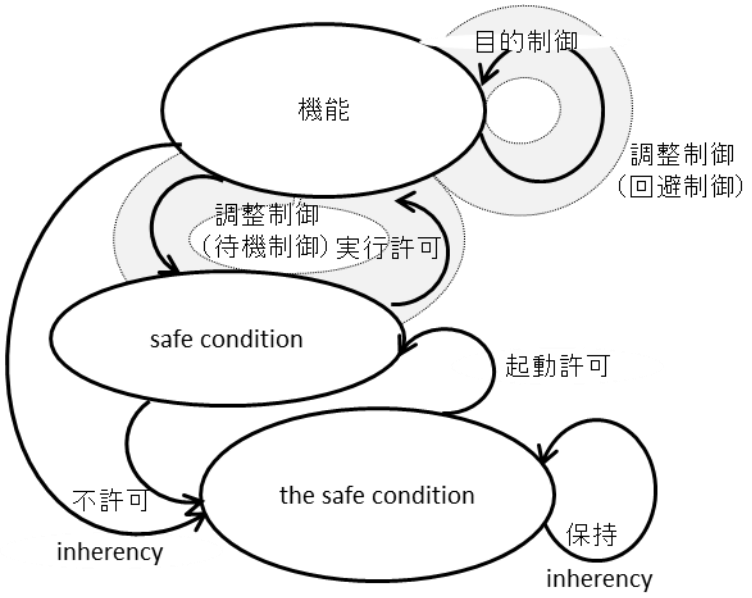


Fig. 5 － 3　安全システムの構成

５－２－２　調整概念

自律性（制御性）が確保されるのが安全の中であるが，そこには自らを自らでもって制止するという自己インターロック概念がある．自律ゆえの概念である．これは，精神構造における超自我・自我・イドの超自我として見ることもできる．超自我とは倫理や道徳的判断基準により裁定を下す機能であり，自我とイドの統御的存在である．イドとは本能的エネルギーとしての目的実行の駆動力である．そして自我とは超自我から禁止の裁定が下されないようにイドを調整している機能である．この調整能力があるからこそ自己意識が芽生えると言われる．倫理による裁定者（実在する人間ではない）との関係性により生じるのが自己であり，調整するまたは抑制するというところに自身を認識する．一般に，良心は倫理によって鍛えられると言われるが，この調整概念こそ良心的位置付けである．そして超自我がないところに自我は規定しえないのと同様に，限界に対し禁止しえないとこに調整概念は規定しえない．この調整という概念があるからこそ，自らの制約を認識し，その限界において超えないということを確実にすることを求める．そして能力の限界においてインターロックを求める．調整とインターロックは相互に規定しながら，また形成するものである．

人間の意識するものにおいては機械においても作業においても，この制御形態としての

構造が本来的であると考える．機械が目的機械とインターロックだけで構成されているとき，そこに人間が調整制御を行っていることを認識する必要がある．インターロックがないときも，人間がインターロックを行っているのである．これらがないとき，単なる欲望のままに行動する人と，その機械・作業に違いはないと言ってもいいのではないだろうか．

５－２－３　人間の安全確認と調整作業

誤りのない Se=1 を要求するのは信頼性に基づく安全だと一般に理解される．残る不安から Se=1 の根拠 Sc を明かにして，Se=1 に代わる Sc=1 の方がより確かだとされるような安全確認は本来の「安全」と認められない．例えば設計基準強度 Fc を決めるとき，安全率５で実際に作成することで，信頼性高く作成すれば５×Fc は確か（ここで５×Fc を Se=1 と見立て）であり，それから十分離れている Fc は確実（Fc を Sc=1 と見立てる）に保たれると言うようなものである．それはやはり信頼性の改善を直接志向するに過ぎないからであり，信頼性であり安全ではない．

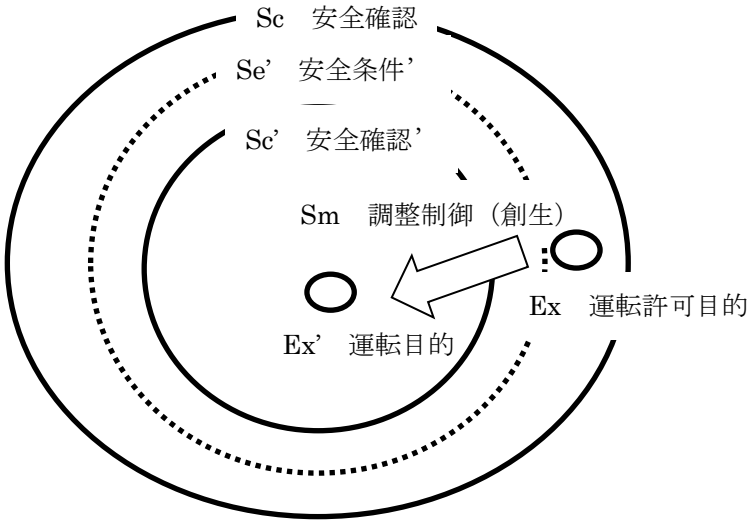
特に制御（情報と操作）において安全を作る場合，その判断基準が重要である．先の信頼性は設備の引き渡しにおいて確認として用いられるかもしれないが，得てして廃棄（停止）においてその判断は遅れることになる．安全に基づく「許可」は，信頼性というより，許可を決定する条件(安全の条件)に対する正当性に徹底的に依拠する．すなわち許可 P は，Sc≧P でなければならず，さらに，安全確認 Sc は Se≧Sc でなければならない．

許可 P は安全条件の一つ一つの確認に基づくもので，許可 P の正当性はむしろ Sc=0 の時は絶対に P=1 とならない構造, また, 自ら勝手に P=1 とならない構造をいうのであって，逆に，P=0 側の誤りは許されるという意味であり，安全性は信頼性とは異なるアプローチである．

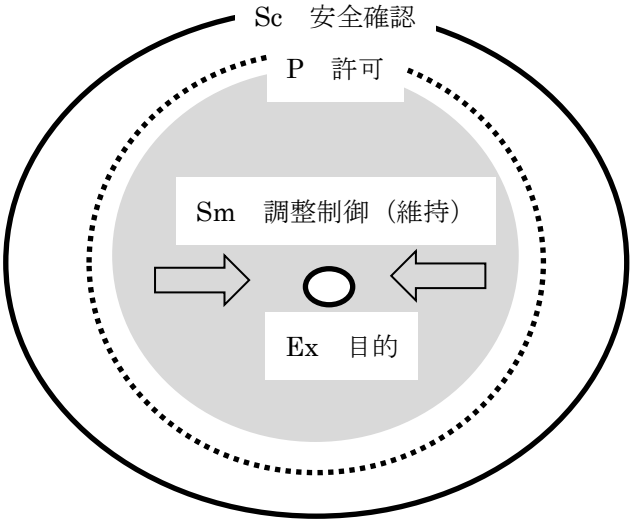
安全確認のこのような構造を無視して人間に安全確認を委ねるケースが多い．安全の条件が曖昧である場合，それが取扱説明書等で示されていても，確認の条件 Sc が曖昧である場合が少なくない．もともと人間に依る安全の判断は曖昧であり，人間が出す許可の判断結果 P には曖昧が含まれると考えざるを得ない．それにも拘らず，事故が起こっていないとすれば，単に，事故が起こるまでの偶然でしかなく，事故に対する不安を解消できない状況は，決して安全とは言えない．

ところで，あらゆる目的に適合した単一の安全条件というのはそう簡単には存在しないであろう．それ故に目的のために階層的に構築していくことになる．本来的な目的としての運転許可が容易に生じないのは，安全条件が確認されない限り運転許可は出ないが，許可を生ずるとしたら，許可を得ることを目的とする情報と操作（制御に類する作業）が実行されており，厳格な判断による許可 P=1 を確保するには，単純とは言えない安全条件の生成・維持という操作が明らかに存在する．

図 5－4 にその調整概念を示している．人間による調整作業として検討してみると，例えば，首都圏の朝の列車は混雑するが，昔は駅員や押し屋が押し込んでドア閉のロック状態（安全の条件）を作っていた．昨今は昔ほどの混雑ではないかもしれないが，安全状態は作らなければできない．慣れた客であるか否かで作業は変わるが，乗客自身が（乗らないことも含め）ドアが閉まることができる状態へと自身を調整することで許可を出すためのドア閉を作り出している．これを実行した後に，改めて安全確認を行えば，Sc=1→P=1 となり，稼働率に雲泥の差が生ずるであろう．すなわち，安全の確認に基づく許可のシステ



A)目的のための安全状態の生成



B)安全状態の中への維

Fig. 5 － 4　安全空間における調整概念

ムを実質的に運用するのは人間であって，調整作業のための人間の存在が前提となっている．そして現在この安全条件を確認しているのはドア閉により生成可能な信号通知である．

またここで，ドアが開いているということは，停止状態が厳密に確保されていることが必要である．そしてドアが閉まったのを確認し，ホームに人が居ない（黄色の線の内側，ホームドアはそれを構造的に達成する）ことを確認し，運転許可が出る．運転実行許可においても，他の列車が前（閉塞区間方式だと，前やその前の区間にいないことで速度許可が出る）に居ないことを確認し進行することができる．先行車両だけでなく，踏切信号やカーブや風雨での速度規制等で許可が出る安全条件が変わってき，その安全条件にあるからこそ進行できる．その安全条件もカーブや踏切はトランスポンダで情報を得ているが，情報を得ることで安全条件生成ができるからこそ運転でき，生成できないときは運転許可とならない．そのトランスポンダが正常であるからこそその安全条件を確認できる．一般に，送受信装置（帯域が同じ場合）は自身の送信機が送ったデータに対し自身の受信機が受けることで送信確認し，異なったデータを受信しだすことで，送信途中に優先データが来ていることを判断し，割り込み対処（送信中止等）する．しかし普段，自分が出しているものを，環境（システム外部）を通し受信により確認できるからこそ，独立した判断として自身の正常性が確認できる．

ドアが閉まるという状態を作るために，乗客は積極的に協力しているからこそ安全条件としてのドア閉での信号が出る．運転士が，新たに安全条件が変わっていってもその速度規制内に事前に抑える制御を行っているからこそ，連続的な運転許可が達成されている．

乗客や運転士の積極的な調整がなければ，列車はホームで止まったままであるし，動き出したとしてもすぐ止まってしまい進まないような状況になるはずである．止められてしまう前に，止められないように積極的に調整しており，機械よりも人間が得意とするところかもしれない．また逆に，むしろそれ故にと言ってもいいかもしれないが，止める判断は人間には苦手であり，むしろ機械の方が正確（人間から見ると冷酷に）に処理を行うことができる．

本来，一人の人間が行う行為として，5－2－2 節でも挙げたイド・自我・超自我的な分類として目的・調整・確認（監視）が挙げられ，それらを総合的に実行していると考えられる．しかしこの超自我つまり確認（監視）においては絶対的な独立が必要になってくる．得てして自身がこの 3 つのそれぞれを行っているということは忘れられがちである．そして 3 つの作業を独立的に行うということは，一人の人間であるが故に難しい．目的に集中するとは，調整・確認（監視）への注意がいかなくなることである．目的を「うまく行う」ことに気が行き，それが“安全に”行われているかに注意が行かなくなる．また，特に調整を行っている場合に注意が必要であり，確認で OK が出るために調整したのだからと，調整作業をしたが故に確認作業が省かれてしまう．本来，安全の条件を整えるためであるにもかかわらず，調整作業の「ついで」の感覚で人間が確認の役目を担ってしまうのは，確認でなく信頼性に安全性向上の重きを置く見方からは自然であると言える．

Sc=1 を目標とする調整作業を終了して改めて Sc=1 を確認するのを，調整作業を行った本人が行うことは難しい. 調整作業で必ず Sc=1 が確保できるとは限らない. 情報と操作（制御様の作業）による目的は必ずしも達成できないから（信頼性依存），改めて，安全の確認が必要である．したがって調整作業には，改めてこれと独立の条件で安全の確認がなされなければならない.

あらためて，Sc=1 を目標とする人の調整作業 F(Sc)とそれで生成される安全を同義と見て Sm(=F(Sc))で表すと，調整作業 Sm(=F(Sc))≧P と Sc≧P が独立に実行される．そこにおいて安全確認 Sc≧P に基づく判断結果 P が優先されるということである. ここにおいて，同時に実行されている Sm(=F(Sc))によって，Sc≧P の正当な P=1 が高い確率で得られ，この許可を受けて，機械の運転が実行され，高い稼働率を得ることができる.

この様に安全条件を生成しそれを維持するということにおいて，安全条件に入れるための調整，安全条件から出ないための調整が行われているからこそ，安全確認による運転許可は生起・持続される.

５－３　制御概念

５－３－１　調整制御の概念

私たちは普段，事故を想定し，“そうならないように”と制御を行っている．自転車においても，目的地に向かうのとは独立して「倒れないように」と制御している．そして倒れる前にブレーキを掛け，足をつき止まる．この「倒れないように」というのが調整制御であり，この制御により，事故（転倒による傷害）を避ける処理と目的地へ向かう処理が融合する．これは産業機器の制御でも同じである．たとえばプラントで爆発性物質を扱う場合でも，爆発を事故と定め，爆発温度が与えられると，そこから離れた温度で処理を行う．そのとき，爆発温度になる前にシステムを停止し爆発を回避するが，それに先立って，爆発温度にならないようにという調整制御が入る．この確認作業は連続的に行われる必要がある．ゆえに意識的にはその継続に無理があり自転車なら潜在意識下に習得されるが，プラントを潜在意識で見るわけにもいかずまた意識的に常に見続けるという行為は人間にはできず，機械に頼ることになる.

単なる調整（目標値－制御値＝０）であれば，いたるとこで行われている．ここで注目しているのは,「そうならないように」という調整であり, 事故の想定の手前に目標値を置き，その目標値は何が何でも超えてはならないとする制御である.

また，もしブレーキのない自転車なら転倒傷害を覚悟してスピードを上げなければいけない．また，停止構造（操作的保証）がない爆発性プラントであると，その影響が及ぶ人々の相当の覚悟が必要になる．この時の調整制御は非常に厳しい要求のものになる．ある意味機能安全をここに持ってきて認証されれば OK とするところがあるが，そもそも「止ま

れない」機械を作る必要があるのかが問われないところに問題がある．

調整制御は事故を想定し事故にならないようにと制御するが，しかし安全としての確実さを求めると，事故になる前に安全に止まるというシステムを構築することで，「止まらないように」という，実行許可へとつながる積極的な調整系へと変換される．

５－３－２　安全制御システム

安全な機械があるわけではない．安全に運転する制御が存在し，私たちは，それを忠実に実行することで事故を防いできている．安全は信頼に足るものでなければならない．安全性は，低リスク状態を維持する目的で実行される制御（行為）の信頼性（評価）だという見方もできる．ここに制御とは情報に基づく操作によって目的を実現しようとする概念である．事故を情報（想定し予測する）として掴み，その回避を操作しなければならない．事故へと遷移する前の制御可能な指標を掴まなければならない．事故は，人が危険源に暴露された状態（危険状態）で発生するとされる．事故を防ぐということは，危険状態を予測し，これを回避する制御を行うことである．この制御をここでは危険回避と呼ぶ．人間が危険源に暴露されない条件（安全条件）がある場合，事故を防ぐために，安全条件を維持する制御を行うことになる．この制御を，安全制御と呼ぶことにし，危険回避と区別する．もともと機械には合目的的機能が与えられ，人の操作，自動制御のいずれによらず，情報に基づく独自の操作が実行される．事故は，合目的的機能の実行に伴って危険状態が生じたのに気がつかないまま制御を継続することで発生する．危険回避（または安全制御）は，危険状態を生じない条件で合目的的制御の安全を確保しようとするものである．そこで，危険回避（または安全制御）の失敗によって必然的に生ずる危険状態に対して運転（合目的的制御）を停止させる必要が出てくる．インターロックと一般に呼ばれるが，危険状態の回避を断念して停止操作を行う“制御”と捉え，ここでは停止制御と呼ぶことにする．

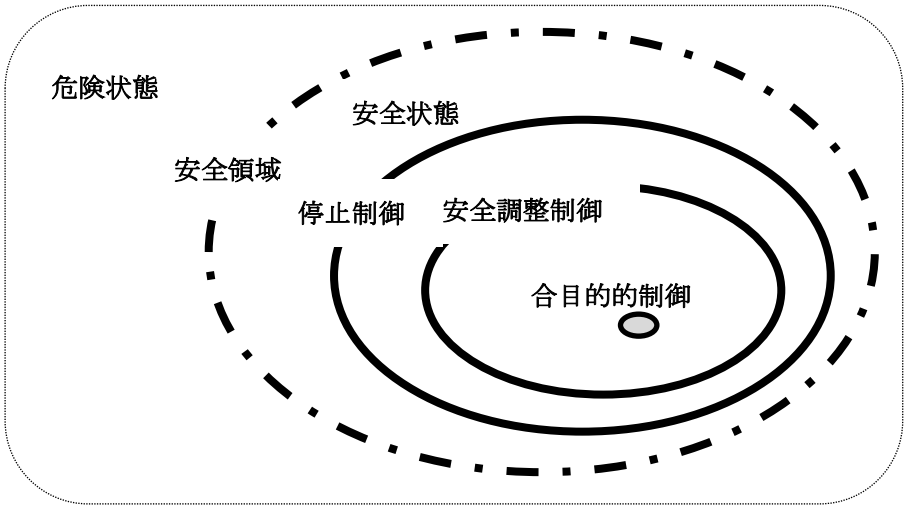


Fig.５－５　安全制御システムの構成

これを概念的に示したのが図 5−5 である．危険状態へ至る逸脱を階層的に回避するシステムである．今回，危険状態回避の目的にて構成された安全制御システムを 3 つの制御において提示する．

５－３－３　安全制御システムの構成

事故は危険状態になり，そこで危険事象が発生し危害へと繋がる．危険状態回避の目的にて構成された安全制御システムを 3 つの制御において提示する．これは安全状態維持を目的としているともいえる．

Ⅰ：合目的的制御

目的により制御（情報・操作）が規定されるとする一般的な制御である．また先の信頼像で示される合目的能力における制御であり，目標としては危険状態以外の具体的点で示される．あえて危険状態に目標が定められることはあり得ないので，合目的的制御の実行過程で危険状態が生ずるとしたら，外乱(ノイズ)によって目標が変化した場合，あるいは，それまでの目標位置から次の目標位置に変化する場合に定められた経路を誤って逸脱したという場合である．

通常，“安全な”環境条件が設計された制御である．目的まで至るルートは安全領域の中に引かれ，安全領域（情報）を定めてそこで運転（操作）しているのは当然であり，正確にもって実行されれば危険状態にはならない制御である．これは一つの目的に向かうということによりその形態が規定された単独の制御である．

Ⅱ：安全調整制御

危険源が存在し，危険源にさらされることで危険状態となり危険事象が発生する．そしてこれが結果として危害へとつながり事故となる．この事故となることを避けなければならない．危害・危険事象・危険状態・危険源，それぞれに「情報」が得られて「操作」が可能な手段があれば，事故回避のための制御が可能になってくる．事故となることを避けるための制御が必要になってくる．

危険状態になるということが捉えられるなら，予測し回避する制御を行う．そして危険状態にならないという条件がわかれば，事故を防ぐということは，その条件をもって安全状態を明確に作り，その条件を維持する制御を行うことになる．安全調整制御が安全状態を創出しているといえる．

それが，合目的的制御で求められる“安全な”環境条件である．安全に関して，事故を回避する確固たる制御が求められているが，合目的的に危険状態の回避が強く要求されて

いる．合目的的制御の危険状態への遷移可能性を排除し，合目的的制御を安全状態に保つことを目標に制御が行われる．合目的的制御の実行過程で危険状態が生ずるとしたら，外乱(ノイズ)によって目標が変化した場合，あるいは，それまでの目標位置から次の目標位置に変化する場合に定められた経路（情報・操作）を誤って逸脱したという場合である．合目的的制御の実行過程での危険状態へと繋がる誤った逸脱の情報を捉え，安全領域の中で，安全状態に維持しつつ，本来の運転領域へと戻すべく調整（操作）がなされる．

危険状態になるという「情報」，つまり安全状態を定めた条件を壊す要因は，主に外部から安全領域そのものを壊す要因と，主に内部として安全領域を逸脱する要因がある．そして危険状態にならないという条件を「判断」に，その条件の確保を「操作」し続ける制御となる．そしてこれが安全状態を維持する安全調整制御である．この操作は危険の対象と主体を分けることでもあり，この操作により隔離としての安全状態が維持される．

Ⅲ：停止制御

停止制御は危険を判断したときにシステムとして停止安全状態へ移行するものであり，それゆえ目的制御も停止する制御である．危険源をエネルギーとして用いている合目的的制御が安全状態を逸脱することに対し，目的制御への強制的介入制御である．

安全調整制御で安全を能動的に確保している状態の正常性を判断し，異常と見た場合は安全領域の中で合目的的制御を停止する制御である．目的制御に情報として与えるのではなく，外部から目的制御の資源への操作により目的制御実行を不能にすることである．具体的には危険源への介入になり，危険源のエネルギーに対する遮断行為である．停止制御は合目的的制御の実行を停止状態に移行させるに当たり，適切な着地レベルを「情報」として見極め，そこに向けて着地のために資源を「操作」する．

５－３－４　3 つの制御の連係

事故回避には失敗は許されない．この失敗を回避し無くすべく，合目的的制御，安全調整制御，停止制御，これら 3 つの制御は連係している．そして，合目的的制御の逸脱に対して確実に危険状態を発生させないための安全システムとして組まれる．そして独立した関係であることで，危険状態回避に関して連携した関係と言え，評価としての回避可能性を格段に高める．

合目的的制御は目標点での制御であり，定められた点・線上の偏差を無くすべく操作される．しかし，外乱や制御エラーがある．これによる許容できない偏差を捉えるべく，安全調整制御は“範囲”での制御を行っている．一つは外乱を排除し，安全領域を形成すべく制御を行っている．もう一つは，許容できない偏差が出るのを捉え，許容できる中に戻していく．さらに，安全調整制御で抑えきれない，または安全調整制御のエラーが重なっ

た場合を捉え，停止制御が控えている．これは絶対的制約のある制御である．事故を危険により定め，危険となるその前にリスクとして確実に発現しない状態にしなければならない．合目的的制御による偏差が危険（許容限界）に達する前に停止させなければならない．逸脱能力と停止能力の関係より，危険を前に確実に止まれるところに判断点は置かれる．現在の認識空間からその空間を差し引いた空間と（逸脱可能の）能力との関係より最大許容時間を確保しそれが仕事に供される時間となる．また再度確認することによりその時間はクリアされ，その連続が時間性となる．そしてその許容時間の遅れ（次の確認の遅れ）は許されないとなる．

これらの３つの制御は目的が違い，見るべき情報が違う．そして自らの正常性の逸脱としての失敗は自ら判断できない．自らの見えないところを，見てそして解決すべく次の制御がくる．例えば，空間的制御はその失敗が空間的逸脱として捉えられる．システム外部の環境に現れる結果を捉えるからこそ，そのシステムと独立していると言える．ゆえに独立につながることで，できないことをきちんとカバーする関係が生まれてくる．これら，各制御の「できない」ことに対して，それを「できる」制御が独立して連携しているがゆえに，危険状態回避という要求に対し，明確な対応により最後まで問題を残さない．そして安全調整制御が安全状態を維持すること，そのことは安全調整制御の正常性が，合目的的制御の実行許可状態を担保していることである．

これらのことは，安全性は，低リスク状態を維持する目的で実行される制御(行為)の信頼性(評価)だという見方もできる．上記 3 制御は「できない(制御エラー)」状態に対して，そこに「できる」制御が入るということで，独立にかつ連携する．故に要素構成が独立ならばシステムとしての危険側故障率(不信頼性×危険側非対称故障特性)の評価は，各制御の危険側故障率の積の形をとる．

５－４　安全監視システム

事故回避には失敗は許されない．この失敗を回避し，無くすべく，合目的的制御，安全調整制御，停止制御，これら 3 つの制御は連係している．この連携により，監視調整制御としての上位層概念を持つ．これは監視制御としての階層構造を持つ．合目的的制御はこの安全の中に目的が定められている．監視制御は，安全を確認し，確認できなくなれば停止制御を行う．安全調整制御はこの監視・確認されている安全の中で，合目的的制御が監視から出ないように抑制している．ゆえに監視制御は安全を知り判断ができるといえる．

合目的的制御による偏差が許容限界を超えるのを前に確実に停止させるために，これら各制御は「できない（不能)」状態に対して，そこに「できる（可能)」制御が入るということで独立にかつ連携している．危険状態回避に関して独立に連携するがゆえに，危険状態回避要求に対し，最後まで問題を残さない明確なシステムと言える．システムとしての危険側故障の評価は，各制御の危険側故障確率の積の形をとる．そして技術者はリスクとし

ての要求に対し，具体的行為（制御）を正当性と確率でもってリスク評価に供することができる．

この安全調整制御により安全制御システムのシステム特性が構造として明確化される．安全調整制御により，合目的的制御のエラーが修正され，運転の信頼性は向上する．また，停止制御の要求を減らし，安全における信頼性も向上する．これは，安全調整制御により安全(停止制御)と運転(合目的的制御)に対する冗長構造が組まれることでの非対称特性による．システムに対して信頼性・非対称性・冗長性としての安全特性を持たせるのが安全調整制御である．

車など，ある速度に対して，停止に必要な距離(安全空間)が確保できてこそ，その速度が出せる．止まれることを事前に保証できるからこそ実行できる．停止制御は安全確認の正常性である．安全調整制御は停止制御による安全確認された中での正常性を示す．そして安全調整制御は安全確認された中での運転安定性を示す．安全かつ正常な中で目的への復帰・調整操作等が行われる．そして安全調整制御が安全状態を維持すること，このことは能動的(信頼性)な安全確保の正常性が，合目的的制御の実行許可を高い稼働率で担保していることである．

これは危険状態の発生を徹底的に許さないという要求に対して，危険状態の発生可能性を徹底的に排除していくシステムであるが，それは実行許可を作りだし運転条件に戻していくシステムでもある．そして 3 つの制御は連係により，３つの制御に対してメタ・ポジションとしての安全監視システムとして安全確認は行われる．

５－５　安全システムにおける停止

５－５－１　安全システムにおける停止と運転

仕事と事故回避，この 2 つを両立させなければならない．これは，

：目的(仕事)達成に対して合理的なシステム，

：また結果(事故回避)が常に達せられることに対して合理的なシステム

である必要がある．この 2 つが独立に融合するのが安全システムである．安全システムは，運転の逸脱を入力とし，運転・停止の判断基準を持ち，運転継続状態と停止状態を出力として確実にするためのシステムといえる．

事故を予測し，そうならないように操作を行う．目標を事故に定めるが，目標の否定操作である．偶発的作用で事故の方向へと変化するのを捉え，事故から離れる方向へ操作することである．ここで事故の予測から離れすぎたら危険を捉えることができなくなる．安全を認識しているとは，事故を危険として捉え，かつ事故から離れていることである．常時危険を捉えているからこそ，事故から離れて安全であるのが分かる．これにより安全システムの形態ができる．それは定められた安全領域の中に保持していくことであり，事故

から離れる制御で安全保持形式が取られる．仕事をするために安全領域を作っていく．そして領域内への保持という形式をとり，空間の中で領域内に留まる非対称性を持つ．この形式において，信頼性を高めれば安全性が高まる．

しかし作用は偶発的であり，故に回避には失敗の可能性が付きまとう．危険状態へといつどのように逸脱するかわからない．回避するときには危険を正確に捉えなければならない．基本的には真に危険な状況とは，分からなくなったとき・制御不能になったときともいえる．また，大きな危険エネルギーを持つ機械ほど大きな危害へと繋がる可能性が高く，逸脱の可能性をより強く制限することが求められる．これは領域保持を多重に行うのではなく，領域保持の限界に対して，新たに独立した操作を行うことが求められる．

基本的に，危険への対処の限界，または分からないという状況が来る．このような時，方向性・操作性を問わないのが停止操作である．これが運転調整システムの境界での停止制御であり，目的制御の停止である．運転調整システム境界で行われるからこそ，仕事の目的とは独立に共存できる．この停止制御により，安全領域からの逸脱抑制に対して確実性が高まり，またこれは逸脱エネルギーの低減操作でもある．そしてこの停止制御により，システム境界が際立ち，安全システムのシステム特性が明確になる．安全システムは，事故回避制御から新たに安全領域境界に対し止まることの合理性を明確にし，また運転(仕事)に対し，止まらないようにという運転保持形式の調整制御構成となる．

５－５－２　停止の共通性

想定したものに対して想定通りに対処するのが安全の問題である．人間は，分からないという状況を認識し，新たな問題の発生を発見（想定外に対処）できる可能性を持つが，安易に人に危険を委ねてはいけない．そこにおいて本来の，想定に想定通り対処することがおろそかにされる傾向がある．そして，想定通り対処することには「停止する」という共通性がある．これは逆に，停止状態を安全とするという共通性でもある．

停止制御は様々なリスク事象に対して共通性を持つが故に，分からなくなった状況，新たな問題を認知した段階において，被害を低減する可能性がある．機械においては自らが持つ危険エネルギーが害をなす．加害を与える側にしては，その自らのエネルギーを自ら消散させることは，加害の可能性に対し共通する対処である．また，安全システムの限界において，強制停止としての非常停止を委ねる(停止の能力を持たせる)ことで，人に危険の可能性を委ねることが検討できる．

これは不確実性(新たな問題, 想定外)への対処（機能）の可能性として注目してしまうが，そうではなく，システムの健全性（構造）として考えるべきである．少なくとも，自ら使用する危険エネルギーにおいてはそれを消散させることができるから利用可能である．

Eout= Ehzd・N*

つまり正常時以外―N*は OFF（Eout＝０）となる特性（構造）を持つ．（図 5－6）

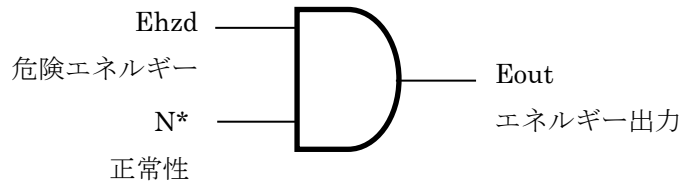


Fig. 5 － 6　危険エネルギー使用のフェールセーフ要求

５－５－３　運転停止のリスクと階層

事故も運転停止も事業に対するリスクである．即座に運転再開ができる停止が最も被害が小さく，また事故による事業停止は非常に被害が大きいといえる．安全は事故を想定し，想定通り回避することである．安全システムは事故を停止により回避する．そして，運転システムは「安全システムによる運転停止」のリスクを避けるシステムである．停止制御に対し，もっともリスクの小さい停止を指向するため自らを調整する．

危険なエネルギーを用いて仕事をする場合，逸脱への対処として確実なのはそのエネルギー出力を停止し，事故とは離れた状態にあることである．しかし実際として常に確実な停止ができるわけではない．安全な領域を出る前に確実に停止を目指すのが，エネルギー・ゼロを目指した制御であり，エネルギー処理の問題が伴う．時として安全領域を逸脱して危険状態へと突入し，危険事象が発生する．ここにおいて新たな危険状態に対し制御しなければならない．危険事象が受け入れられない事故となるのを回避しなければならない．

安全領域からの逸脱時，最悪事象（システム外部への被害）を回避するため，（システム内部において）犠牲を払ってでも停止を確定させなければならない．故に，停止の逸脱には犠牲が伴う．それは自らを破壊してでも危険エネルギーをより新たに制御可能な状況へとつなげ，例えば，火事においては生産に重要な設備を壊すことになっても，外部への延焼を回避すべく，スプリンクラー等で消火剤を撒いたり，可燃物等の破壊除去で抑えたりしなければならない．停止制御の失敗という安全上のクリティカルな問題に対し，事故事象における被害の非対称性を確保する“抑制”が重要である．それはたとえ自ら被害を受けても絶対に加害者にはならないということを確実にする信頼の完全性を達成することでもある．そして，停止の構造はその危険側故障である被害の非対称性確保で規定される．被害の非対称性で停止の構造が，停止の構造で調整制御が，調整制御により目的（運転）制御が規定されていく階層構造であり，それゆえに危険側は逆の連鎖である．

例えば，圧力容器はその耐力に限界がある（図 5－7）．能動的に許容圧力内で停止させることができれば運転再開が容易で望ましいが，能動的停止制御の失敗で圧力上昇する場合がある．設計最大許容圧力を超えることはデザインベースの危険事象であり，真の耐圧限界を超えるとき制御不能な危険事象となる．これに対し，能動的停止制御の失敗が最大許容圧力を超える前に受動的停止が行われる．電源ダウンでのエネルギー供給の停止であり，

開放弁での圧力エネルギー開放である．許容圧力内であればその圧力での一時停止（目的制御への指示）でよいが，圧力開放制御は，目的制御が停止できないことへの強制介入である．そして真の耐圧を超えたとき，容器破裂に関しても，防護壁によるカバーにより，危険事象のコントロールが行われる．カバーによる破片飛散防止や，防火油槽による漏れ処理，毒性の場合は隔壁による漏えい防止，または問題はあるが希釈での大気拡散（公害は外部に放出することで生じており，アスベストも労災防止のための外部放出により周辺住民に生じている例もある.）などである．これは，危険事象のコントロール下での発生といえ，危険事象を新たに操作対象として防御が行われる．また，これらの危険事象の段階を捉えて，退避などの危険回避行為が行われ，事故事象の軽減を行う.

危険事象に対し，停止手段・停止リスクがあるが，それが前倒し（階層）的に構築されるのは，運転再開容易さ等で評価される故である.

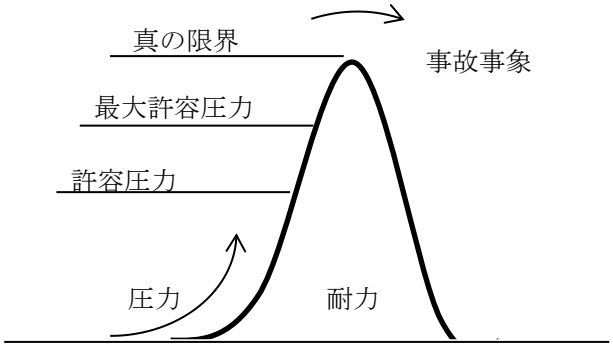


Fig.５－７　圧力容器耐力モデル

５－６　企業体と安全における認証

５－６－１　企業体（組織体）維持としての安全

企業は社会においてサービスを提供する.技術者はマネジメントの実行に応えることが要請される．もし生産性が大事なら，その要素となる労働・物的資産・資本を守る意思がないと守れない．目的に向かうことと同時に目的から外れないことが重要である．無理をして事故を起こすと，事業の存続自体が許されなくなる.

しかし「間違いは人の常」である．だからこそ，その間違いを社会としてどう受け容れていくか，と提起され，社会を納得させることが重要になる．労働・物的資産・資本の安全を第一に考えるということは，生産を守り生産性向上に向かうためである．そして安全は人命等に絡んでくるが故に失敗は許されない.「取り返しがつかない」がゆえにそれを防ぐという制御が必要になってくる．逆に金銭等の取り返しがつくものは，起こってからの対処も可能である.

また，事故は制御不能において認識される．しかし，制御不能になってトラブルの存在を

認識しうるのは人間のみである．そして危険を想定外ゆえに何の対処もないまま人間に委ねるのには問題がある．危険への対処を委ねるからこそ，そこにおいて人権への配慮が強く求められる．委ねる側と委ねられる側の「信用 trust」が重要になる．

信頼関係を相互に形成するが, 現実には期待が裏切られ被害が生じるような状況が起こりうる．このとき，不慮の結果 accidental event であるとき，信頼関係の喪失を防ぐための合意の可能性を見いだせる．例えば, 被害を最小にする最善の配慮（state of the arts， best effort principle etc.）を行った結果としての被害を受け入れるというように，信頼関係には不慮の結果に対する受容のための合意（事前責任と accountability）が得られていなければならない．このような状況において偶然の事故 accident として被害者救済のための保険が可能となり，加害者・被害者ともに救済される．

社会として認める原理・原則から，社会にとって合理的な説明が必要になる．安全とは明確な禁止と表裏であると言ってよく，それゆえ様々な原理を整合させるガイドラインとなるのが「安全とは実行（運転）の許可を出すため」である．

５－６－２　事故を防ぐ制御

様々なトラブルが生じ，それが回復不能(制御不能)な状態へ遷移するとき，事故と認識される．作業者にとって事故は病気・死傷といった傷害となり，その防止が善管注意義務として経営者に課される．経営者にとっては個別の事象で労働・物・資本が毀損するというだけの話ではなく，経営体そのものが失われる可能性を認識することになる．事故になってからでは手遅れである．事故を経験するわけにはいかない．経験する前に回避することが必要になる．

しかし経営者が責任を果たすためにと，一人ひとりを直接監督することはできない．委ねてかつ自らのコントロール下に置かなければならない．そのとき認識される評価対象がリスクとなる．

技術者には「事故にならないように」という制御が要求される．事故は自然には回避できない．必ず回避できるとは限らないが，少なくとも回避を目的とする制御を行わなければその可能性は得られない．先に出した例において，自転車では足をついて止まっている状態，加温プラントだと熱源の供給を遮断した状態，我々はこれを安全な状態と見るはずである．仕事は停止しているかもしれないが，仕事を放棄して止まるわけではない，運転再開のために行っている停止である．事故が起こると組織体自体が失われる．労働者に最後を委ねるというのは，事故の中（停止しない状態）に飛び込むことではなく，たとえ事故の後であっても“停止”後の運転再開で仕事を継続することを求めている．仕事に積極的な労働者がいるからこそ，事故の前の停止という安全状態が意味を持ってくる．

「事故にならないように」という制御は，事故から離れた安全な仕事領域を見つけると，離れているから安全という制御ができる．その安全限度において，たとえば停止という“安

全状態”に移行する，という構造が保証されると，たとえそこが仕事にならなくても，少なくとも事故の心配をする必要はなくなる．そしてその領域へ入ることを避けることになる．「事故にならないように」から「止まらないように」への変換である．そして「止まらないように」に積極的・能動的な制御（調整制御）を組み入れていくことが，本来の仕事に向かうための運転許可を積極的に出すシステムとなる．

５－６－３　安全における要件及び停止構造

経営者は事故につながるトラブル処理を労働者に委託するが,制御不能状態の想定で人間に確実に委託できるのは停止操作であり，またその操作が可能な環境であることが必要である．火中で消火活動をさせるわけにはいかない．

経営者は技術者に，制御不能状態が安全側であることを徹底的に要求し，そこにおいて労働者に危険側における非常停止を委託する．具体的には事故の前に止まることであり，事故という明確なものを見据えているからこそ，止まることに躊躇は許されない．通常，安全側だからと「故障は止まる」とする．しかし危険を明確にしないとこにおいては，そもそも危険がないのに「止まる」ということに理解がなされない．リスク（危険）を認識しない職場においては，フェールセーフは受け入れがたいであろう．

事故を危険により定め，事故をあらためて制御可能な対象（危険）として捉えなおすことが求められる．そして事故の前に止まる停止処理を構築することにより，事故はあらためて想定事象として見直され,「そうならないよう」に制御が行われる．そこにおいて，危険を明確に定めたフェールセーフ（停止）と，停止を明確に定めたフォールトトレラント（停まらないように）の関係で構築される．そのような構造において，制御不能として制御の限界を超える危険側の評価(確率)が示される．経営者において,残るリスクとして評価され,改めて労働者への（リスク依頼ではなく）具体的な危険時操作依頼が行われる．

技術者が経営者に求められるのは以下である．

① 事故を想定し，そうならないための制御
② 危険側故障の最小化と残留ハザードの明確化
③ 正当と認められる手続き

規格・認証で求められているのは②，③である．マネジメントがリスクとして扱うための前提である．リスクは社会的契約に関わる指標である．社会が受容する条件でリスク低減が図られる必要がある．ここで手続きの正当性として

１）安全確認 confirmation,
２）妥当性確認 validation,
３）検証 verification,
４）認証 certification,

この４つの確立が安全認証として求められる．そして危険側故障が確率としてリスク評価

に供される．ここでフェールセーフ化が求められ，その限界としての危険側故障が問題にされる．危険側故障は信頼性・非対称性・２重化(duplication)等で評価される．信頼性が高いことは必要であり，そもそもよく故障する製品は使用されない．しかし，評価対象は“稼働率”ではなく“停止安全状態”に対する妥当性である．安全側故障は回復可能であり，真に避けなければいけないのは危険側故障であることが明確に評価される．その上で残ったハザードが労働者に委託できるかどうか，どのように委託するかが検討される．

５－６－４　停止構造に求められる確実性

安全は，安全条件を定め，確認することである．確認されることで実行が許可される．日本では「安全」というと，「事故を起こしてはいけない」という観念が一般的にある．安全対策として何をやっても「事故を起こしたらお終いである」という印象がある．つまり，安全対策の結果としての事故が解決されないが故に，結果としてどうなるかわからないのであれば，事故の頻度を減らすことが評価になる．これまで日本は，「事故を起こすわけにはいかない」という強迫で追い詰められた結果として，「事故がないから安全」であったといえる．これに比べ，欧州の認証・保険のシステムは，事故処理においてクローズさせるシステムであり，事故が起こるとどうなるかわからないという不安からの解放である．自由貿易を成立させるには国境を越えたトラブルを回避しなければならない．このための制度が認証であり，保険の条件でのトラブル回避である．そして認証においては害をなさない確実性の証明が求められる．

安全は事故がないことではない．安全は仕事の実行のためにある．人命・環境・その他を守らなければいけない，しかしそれは仕事を守ることでもある．生産のための大きなエネルギーの出力は，危害への発露を抑制することで社会に認められる．安全は停止構造における妥当性であり，故障・エラーが事故に繋がらない非対称特性であり，その構造において信頼性が安全性に関係する．仕事を守る安全システムにおいて運転停止構造の確実性こそ認証において求められることである．

５－７　小括

事故のない状態は，必ずしも「安全」ではない．事故は，危険の状態(スレッショルド)によって予測される．危険を伴う機械やシステムは，危険の状態を制御(監視調整制御)し，一定の未来に事故の予測状態を維持することで事故を防ぐ．本章では安全調整制御の概念を提示し，これが合目的的制御・停止制御と明確に区別されることを示した．安全調整制御と停止制御の関係は，

システムの原因（危険源）を規制する（調整制御）

システムの結果（停止状態）を規制する（停止制御）

という原因・結果の因果構築である．それは式（5－1）のユネイト性（単調関数）としての結果（停止）を確実にするための原因の調整である．それ故に「停止へとまだ遷移しない状態」であり，安全調整制御は積極的に実行許可を出すための制御でもある．

制御には誤り(限界)が避けられない．ゆえに誤りに対し階層化された構造を示すことで，制御システムとしての信頼性の高さ，安全およびリスク低減の関係が明確化される．監視制御システムはこの目的制御の出力により誤りを監視している．監視空間の中で誤りの方向性（安全領域に留まる方向と逸脱する方向）が明確になる．それゆえ調整する方向，その失敗も明らかになり，停止制御にゆだねられる．しかし，停止制御にも誤りはある．「事故の前（監視空間内）に止まる」に対し，「事故の前に止まれない（監視空間逸脱)」という誤りである．そこにおいて人間の非常停止操作にゆだねられる．ただし，人間の介入は停止状態（事故による停止も含め，危険の可能性がない状態）を確認して行われるのであり，止まらないシステムの中に入ることではない．

これらの安全を確保するために階層的になされた制御により，その評価としての回避可能性は格段に高まる．そして残った失敗の確率により保険が組まれ，実際に起こった失敗（事故）に対して救済が行われる．保険等，安全システムの失敗をクローズさせるためにこそ，安全は立証が必要になる．それ故，安全は原理によって作られなければならない（杉本，蓬原，1990)．そして停止等の共有すべき安全状態があるからこそ，妥当性の確認ができる．停止制御の証明性（技術者）に対して，その現実的評価（経営者）としての事故の可能性（残留リスク）がある．その事故を accident とする為の認証条件として，１）confirmation，２）validation，３）verification，４）certification，この４つの確立が安全認証として求められている．

あらためて，確固とした停止構造を持つことは，これまで「事故を防ぐ」と様々に行ってきた事故回避制御等を，「止まらないように」という制御で整合することであり，それは生産性の追求への機能的転換になる．安全は停止構造からその展開を検討することであると主張するものである．

第６章　空気圧システムにおける安全の考察

６－１　空気圧駆動システム

６－１－１　圧力システムにおける安全コンセプト

前章までに安全防御システムおよび安全監視システムについて述べた．そしてこれらは境界（制限）に対する停止の確実性において立証されるシステムである．本章ではこの視点から空気圧システムという具体例を取り上げその証明性を検討する．

圧力容器はその容器自身により危険減と人とを隔離している．圧力容器は耐圧限界があり，これが隔離としての限界である．それゆえ隔離を確保すべく，目的制御とは別に，その限界を超えないようにとの制御が行われる．限界を超えることにより危険状態が発生することに対し，超えないことつまり危険状態とはならないことを確実とするシステムが組まれる．これは，限界を超える前に停止を確実とすることである．

そして危険源に対し，危険状態になる前に確実に停止するというシステムが組まれる．そしてこのシステムがフェールセーフであるということは，危険状態になる前に，たとえ故障しても確実に停止するシステムである．たとえフェールセーフであっても，危険状態に入ってから動作するようなものはリスク低減システムでしかない．安全システムであるということは，危険状態になる前に確実に止まるシステムがフェールセーフに構成されることである．

圧力制御システムで問題となるのは圧力の上昇であるが，システムの内部故障はすべて圧力としての結果に出てくるといえる．ゆえにこの結果を監視するシステムが独立に組まれることで，危険側故障を抑制・停止するシステムが構築される．そしてこの監視システムがフェールセーフであることが，危険側故障を解消した非対称特性を持つシステムとなる．

６－１－２　空気圧駆動システムの概要

空気圧駆動システムは，過圧による容器の破裂や高圧空気の噴出，また噴出に伴う部品の飛来あるいは非制御の圧力による過負荷等により人に危害（事故）を生ずる可能性がある．現状の空気圧駆動システムにおける「安全」は，各種コンポーネント（結合部を含む）の強度設計とそれに基づく圧力制御を適切に行うだけでなく，過圧に対して安全弁等（減圧弁，リリーフ弁，ラプチャーディスクを含む）によって外気への放出を行う等，危険な圧力上昇を防ぐシステムを要求する．しかし，制御の誤りによる過負荷，また，それを回避するための安全弁等の故障（例えば弁の閉じ側の固着）の可能性が依然として解消され

ていない．例えば，空気圧駆動システムの圧力調整に広く使用されるレギュレータは，リリーフ弁の役目を兼ねており，そのため安全弁を要さないと考えるのが普通である．しかし現実には，レギュレータは弁の固着等による危険側故障が起こり得るが，そのためのインタロックが構成される例は殆どないと言っていい．また一方で，現状の空気圧駆動システムが，ALARP の原則による許容リスクの見方から，危険側故障に伴うリスクの評価を行って適正な手順に従った安全関連部の設計を行ったとする例（中村他，2013）もまた殆ど見当らない．

すでに，著者らは前報（中村他，2013）において，空気圧駆動システムのインタロックシステム（以降，単に，インタロックシステム）の提案を行った．これは，駆動系に空気を供給する動力調整部の圧力に注目し，“窓監視”の方法で上昇側と下降側の両方の圧力を監視して危険側故障の影響を動力源遮断によって阻止するインタロックシステムの提案であった．当該システムは，安全の妥当性の根拠を安全(確認)の原理（杉本他，1987，蓬原他，1987，杉本他，1988，蓬原，杉本，1990，杉本，蓬原，1990）に置いており，そのため，リスクベースとする制御に関わる安全規格（例えば ISO13849）に必ずしも整合していない．この点，これまで（梅崎他，2001）にも述べられてきたが，これらの違いは，「安全」の根拠を，前者では「危険（故障を含む）→動力遮断」，すなわち狭義のフェールセーフ(以降単にフェールセーフ，詳しくは文献（川西，1971）)とするのに対して，後者はリスク低減手段（安全関連部）の危険側故障の発生確率の評価に置いていることで生じていると考えられる．ちなみに機械類の安全規格は，2003 年発行の一般設計原則を示す ISO12100:2003 で国際的な整合化を果たしている．ISO12100 はタイプ A（基本規格），ISO13849 はタイプ B-1（一般安全規格：特定の安全側面）に位置する．規格はその時代に合わせ表現等が変化していくが原則は容易に変わらないものである．本論においては，規格が内包する一般設計原則が普遍的なことから，変化しないものは成立時がその意図をよく表していると考え，ISO12100:2003 を使用する．一方，ISO13849 は改訂で，使用される部品および安全回路の構造によりカテゴリを定義するものから，確率的アプローチへ（Neudorfer，城，2012）と原則的変更がなされた，これより ISO13849:2006 を使用する．また，ISO13849 は機械類の安全機能（故障がリスクの増加に直ちにつながる機能）の提供において，制御システムの“設計・評価または下位規格作成指針”として参照される．著者らは停止機能の同時故障回避という視点で注目している．

６－１－３　本章の構成

そこで，本章では，改めて，インタロックシステムと国際規格で規定される安全関連部との整合性について検討を行う．安全（確認）の原理は，危険のときだけでなく故障のときも停止して，少なくとも事故を生じえない保証を要求する．そして国際安全規格によるリスク低減は，危険源における危害の可能性の如何によって許容リスクを評価する．一般

に機械の持つエネルギーが危害の可能性となる．停止とはエネルギーの消去であり，それは危害の可能性を除去することである．停止とは危害の可能性のない状態であり，機械は本来そのような停止を持つことを前提とするのが安全（確認）の原理である．国際安全規格は事故防止対象を広く扱っているがゆえに部分的であるかもしれないが，停止安全という概念の上において両論に矛盾はないと結論付ける．そのため，第 6－2 節では，本研究で提案するインタロックシステムの安全コンセプトを明らかにし，安全（確認）の原理に根拠を置く安全確保の妥当性について述べる．次に第 6－3~6－5 節では，安全コンセプトを満たすための安全要件と，それに応えるインタロックシステムの構成について，第 6－6~6－7 節では，インタロックシステムの故障を，危険側だけなく安全側を含めて監視する必要について，及び，フェールセーフな遮断構造について示す．さらに第 6－8 節では，危険側故障を監視する機能として“窓監視”のために採用するフェールセーフな演算素子（フェールセーフを実現する手段として開発されてきたウィンドゥ・コンパレータ（蓬原，1984，蓬原他，1988，蓬原，向殿，1989，坂井，白井，2000，日本労働安全衛生コンサルタント会編，2000)）について示す．第 6－9 節ではインタロックシステムの機能としての評価，さらに第 6－10 節ではインタロックシステムを，機械安全に関する国際規格 ISO12100-1,2（ISO，2003）と制御安全に関する国際規格 ISO13849-1（ISO，2006）の見方からの検討を行い，当該インタロックシステムの国際規格との整合性について論理的に検討を行う．第 6－11 節では，インタロックシステムと ISO13849-1 で規定される安全関連部との相違について特に停止のコンセプトを取り上げて考察を行う．

インタロックシステムは，遮断弁を用いて，故障時，空気圧駆動システムから切り離す構成である．フェールセーフな“窓監視”とノーマルクローズ型遮断構造を有するインタロックにより，空気圧コンポーネントの危険側故障の影響を抑制し，その結果，理想的と言える安全関連部（ISO13849）が実現可能と期待される．本報告は，これらの検討によって停止安全というコンセプトを中心に上記 2 つの安全の妥当性が相互に整合可能であることを示そうとするものである．

６－２　安全コンセプト

リスクを基調とする安全を規定する国際規格 ISO12100 や ISO13849 は，機械類の制限，例えば “使用上の制限”における“意図する使用”，“合理的に予見可能な誤使用”に伴う「事故（危害)」の可能性をリスクで表し，機械やシステムの運用に当って，社会的に容認されるレベル（許容リスクレベル）を達成すべきと規定する．これが，国際規格の安全のコンセプトと解される．ただし安全の制御に関しては，リスクの低減機能を担当する安全関連部の故障はリスク増大を生じさせる危険側故障であることに注目し，国際規格は，安全関連部の故障の発生確率を許容レベル以下に抑えることを要求する．これに対して，本研究で提案するインタロックシステムは，図 6-1 に示すように，安全（確認）の原理に準拠

し，危害の可能性を有する機械的出力が「安全」を許可の条件とし，安全が確認できないとき（故障のときを含む）許可の停止とともに負荷出力を遮断する．このとき誤って危険な負荷を生じさせる故障が危険側故障に相当するが，当該インタロックシステムは，危険側故障の発生確率を小さくするという考え方でなく，動力源を遮断して危険側故障の影響（被害の出力）を本質的に抑制するものであり，このことをもって安全（確認）の原理に基づく安全のコンセプトの特徴と考える．図 6-1 の **M**，**Q1**，**P1**，**P1***，**&***はそれぞれ 2 値の論理変数であり定義及び論理値の内容を表 6-1 に示す．また論理変数は太字（bold 体）で表記し区別する．ここでシステムの論理的検討を行うため状態を 2 値｛1，0｝の論理変数として扱っている．論理値 1 は論理で示す状態が構築できている場合を示し，0 はそうでない場合（1 の否定）である．2 値論理で安全を考えることについては文献（蓬原，2007）に，安全情報とエネルギーの伝達特性の論理的関係については文献（杉本，蓬原，1990）に論じられている．また，付加記号*はこれまで行われてきたフェールセーフにおける表記法に従ったもので，変数で示す特性が設計の段階で決定されて使用時に変更できないことを特徴づける．機械的構造として変化しない特性，または故障が機構的（必然的）にある状態に固定される構造であることを示す．例えば，強度，最大許容圧力はそれぞれ Sp1*, P1D*(本論文の式(6-3))で示される．また，**&***等はフェールセーフに構成されていることを示し，システムの動作状態において正常時に 1 とするが，故障時には 0 固定される．

インタロックシステムの論理的構成法についてはすでに報告（中村他，2013）した通りだが，それは，図 6-2 に示す空気圧駆動システムのモデルを用いて構成するインタロックシステムに関する．危険側故障の影響を動力遮断によって本質的に抑制するインタロックシステムの構成は，ISO13849 によって，危険側故障の影響を含まない理想的な安全関連部との評価が期待される．ただし，安全関連部を安全関連系と言うべきところもあるが，その違いを強調すべきところ以外は，共通に“安全関連部”と記すことにする．

国際規格 ISO13849 と本論における安全コンセプトとの 2 つの異なる見方から安全の妥当性が論じられている現状において，これらが整合可能か否かを検討することが本報告の主要な目的である．

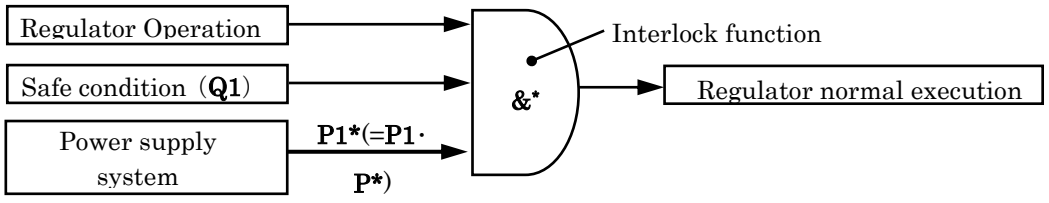


Fig. 6-1 Fail-safe interlock of pneumatic driving system. This model shows a configuration example of the interlock of a pneumatic driving system. In previous report ,(Nakamura, et al., 2013), proposed the design guidelines related to the interlock of the pneumatic driving system which have been studied and proposed based on the principle of safety. From this conclusion, this paper deduces that an interlock to avoid dangerous errors can be realized by shutting off the power supply. Fail-safe interlock is required to bring a system to a halt before occurrence of the hazardous situation by failure of itself.

Table 6-1 Logical variable of the pneumatic driving system (binary logic)

Logical variable	Meaning of a logical variable	Logical variable	Meaning of a logical variable
M	Pressure Operation command	**P***	Fail-safe of the shut-off device
Q1	Being safe (Logical elements)	**&***	State of the interlock function
Q0	Shut-off operational signal (the side of non-shut-off)	**P1***	Shut-off of the shut-off device (the side of non-shut-off)
P1	Pressure control condition		

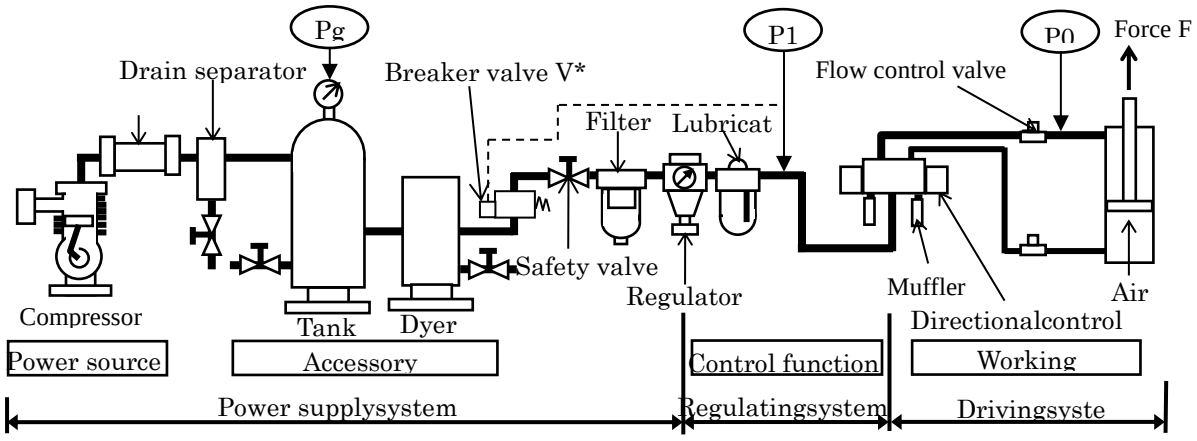
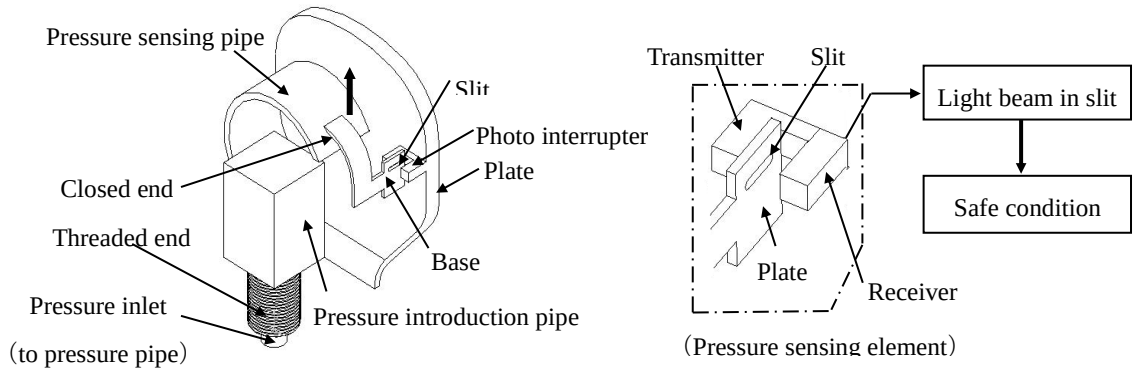


Fig.6-2 Typical configuration of pneumatic control system (Japan Institute of Plant Maintenance



(a)Pressure sensor with window monitoring　　(b)Slid shape spot area for monitoring

Fig.6-3 Method of realizing window Fig.3 Method of realizing window monitoring means (window comparator)

(Society of Safety Technology and Application Japan ed., 2001)

６－３　インタロックシステム

上記のコンセプトに基づくインタロックシステムの論理的構成を示すためのモデルとして図 6-2 に示す空気圧駆動システムが用いられる．ここでは改めてシステムを構成する 13 種類のコンポーネントについて行った故障モード・影響分析 FMEA（Failure Mode and Effects Analysis）に注目する（中村，田中他，2013）． FMEA では図 6-2 のコンポーネントの故障モードを P1，P0 への影響として評価を行っている．ここに P1 は動力調整部の圧力であり，また駆動系圧力 P0 はシリンダの動作により変動するので危険側故障の影響が大きく現れると予想される．FMEA による分析の結果は，P1, P0 への影響として現れる空気圧コンポーネントの故障モードは 220 件に上り，そのうち 15 件は圧力が上昇する側の故障モード(すなわち危険側故障)，140 件は圧力が低下する側の故障モード，残りの 65 件が安全上では直接関係しない故障モードであった．このように数は少ないが，コンポーネントに危険側故障が存在することが明らかにされている．

インタロックシステムは，基本的には，図 6-2 の P1 に図 6-3 のセンサを設置して“窓監視”を行っている．“窓監視”による判断が「安全」を示すとき遮断弁（ノーマルクローズ型遮断弁で図 6-2 の V*）に「開（すなわち“非遮断”)」が通報される．FMEA の分析結果で示すように，インタロックシステムは，空気圧コンポーネントの内，P1, P0 を上昇させる故障モード（危険側故障）の影響を，動力源を遮断して防ぐことを目的として構成される．このときの「安全」の条件は，第 6－4 節で具体的に示されるように，コンポーネントに対する負荷 P1 が許容限界の圧力を超えないことであり，この圧力の限界は，一般にシステムの設計時に最大許容圧力（本論文では式(6-3)の P1D*）として設計者によって規定（提示）される．空気圧駆動システムは，この条件を逸脱しない圧力調整を行って“機能”を安全に実行する．

６－４　インタロックシステムにおける動力源遮断

安全確認形システムは，安全（確認）の原理に基づき，予め事故（危害）が生じないことを確かめて危険の可能性がある制御行為を実行するとするインタロックシステムを構成する．前提として重要なことは，まず，確認すれば安全だと言える条件を明確にすること，もう一つは，それが確認できなければ事故を防ぐための停止手段を確保することである．事故(被害)は機械的出力によって生じるから，“事故を防ぐ”とは危害の原因である機械の操作を停止するだけでなく，動力源を遮断して危害の能力を本質的に消失させることである．しかし，この本質的安全状態をもたらす機能が必ずしも確実でない場合，その不確実性によって生ずるリスクが小さいという判断で安全機能の許可を求めるとするのがリスクベースの安全と解される．

インタロックシステムは，基本的には，第 6－10 節で検討される ISO12100-1,2 や

ISO13849-1 で規定される安全関連部としての要求に準拠している．しかしそれだけなら，許容リスクレベルを達成するためのリスク低減方策と何ら変わりない．もともと人間が「安全」に関わるとき，安全な機械やシステムが与えられるわけでなく，危険を伴う操作を安全に行って事故（危害）を防いでいるのである．安全（確認）の原理において確認されるべき「安全」は安全に使用する条件（“使用上の制限”における“意図する使用”）として設計者によって提示され，使用者はそれに準拠して安全に使用するという関係である．インタロックシステムは，“安全確認を許可条件とする”と言う場合の「確認」には，いつでも停止できる動力源遮断の正常性に対する「確認」が含まれる．また，危険の対応を単なる停止だけでなく動力源遮断によるとするのは，危険時の停止の失敗は，危険の検知と同時に生じた動力源の危険側故障によるからである．しかも，動力源の危険側故障は，重大な危害，すなわち動力源から動力を得て出力する機械そのものの暴走出力となり得る．そこで，リスク発生そのものを阻止するために，インタロックシステムでは，動力源の故障が動力源の遮断となるフェールセーフ（例えば，故障時 OFF 遮断する図 6-2 の遮断弁 V*の使用）の構成とし，危険を検出したときの動力源の同時故障を想定して予め保障された動力源遮断に依拠する「停止」を実行するのである．

以上まとめると，安全確認形システムを実現するインタロックシステムは，次のような条件に従う．

(1) 設計者によって示される“安全の条件”には誤りが許されない．

(2) 安全の確認とは，安全の条件を維持する操作の正常性の確認を意味し，危険を伴う機械的操作は，安全確認を許可の条件とする．

(3) 故障で安全が確認できないときは「危険」と見なして機械的操作を停止する．

(4) 停止には危険側の誤りが許されない．「停止」は動力源遮断を伴い，停止機能の危険側故障の影響を抑制する．

６－５　安全確認の条件

図 6-2 の空気圧駆動システムの仕事出力 F（圧力換算 p）は現実には駆動系 P0 によって実行される．したがって，本来 P0≧p である．P0 は仕事出力の如何で大きく変化するので，より安定した P1 を動力調整部で調節し，これを用いて仕事を実行するという関係である．すなわち，(Pg≧)P1≧P0≧p の関係が成り立つ．ここに Pg は，ユーティリティまたはコンプレッサ等によって生成される圧力源であり，安全システムが別途構成されるので，本論では Pg は誤りのない圧力供給がなされることを前提とする．

一般に「安全率は最大荷重と最小強度とに関係づけられる」と仮定されることが慣習であり（Schuëller，1984)，破損事象の理解としてストレス - ストレングス・モデル（矢川他編，2004)と言われる．今回，空気圧駆動システムを扱い，このストレスとして供給圧力があるが，これは明確に制御可能なものであり失敗を防ぐ対象である．このことを用いて説

明すると，ストレングス(Sp*)がストレス(P1)に暴露される状況において，一般に，ストレスがストレングスを超えると不具合が生じる．不具合を「危害」と見なせば，ストレングスを超えない範囲（すなわち Sp*≧P1）でのストレスは「安全」であると考えていい．もともと不具合(危害)は, 相互の関係で生ずるが, 一般に, 設計時にストレングスが規定され, 使用時に劣化を防ぐための保全（管理）がなされる．これに対してストレスは，自由に調整可能であり，またこのことで危害を伴う誤りが生じ得るのである．そのため，制御の安全では，ストレスがストレングスを超えないための調整を行うとともに，その誤りによる被害を防ぐためにはストレスを監視する必要がある．

P1 の負荷（ストレス）を受けるコンポーネントがストレングス Sci（全部で n 個からなる i 番目のコンポーネントのストレングス）を持つとすれば，次式を満たすとき基本的にシステムは「安全」と見なされるとする．

$$\min\{Sc_1, Sc_2, \cdots, Sc_i, \cdots, Sc_n\} \geqq P1 \qquad (6\text{-}1)$$

ここに $\min\{Sc_1, Sc_2, \cdots, Sc_i, \cdots, Sc_n\}$ は P1 を共通の負荷とするコンポーネントの内の最小のストレングスを示す．ゆえに，最小のストレングスを考慮して，システムとして総合的に定まるストレングス（システム強度）を Sp1*と定める．さらに，空気圧駆動システムの設計では Sp1*を考慮して最大許容圧力 P1D*が定められる．この関係を示すと次のようになる．

$$\min\{Sc_1, Sc_2, \cdots, Sc_i, \cdots, Sc_n\} \geqq Sp1^* \geqq P1D^* \geqq P1 \qquad (6\text{-}2)$$

すなわち，安全に関わる圧力制御とは，P1D*の設定による安全の指針 P1D*≧P1(安全)に準拠して P1 の調整を行うことだと言える．そこで，P1 の出力状態を 2 値の論理変数 **Q1** で表し，P1D*≧P1(安全)のときを論理値 1，P1D*<P1(危険)のときを論理値 0 で表すものとする．P1D*は，P1 が安全であるか否かの判断基準（しきい値）と見なすことができ，したがって, 設計時に設定される P1D*は, 安全 **Q1** を判断する基準として設計者によって示され, 少なくとも危険側の使用に変更されてはならない.

しかし，現実には，安全の指針 P1D*≧P1(安全)による P1 の設定・調整が使用時にも正しく実行されるとは限らない. P1 の調整に誤りが生じ, そのため P1D*<P1(危険)が生じ得る. 一般に，空気圧駆動システムにおける「安全」に関わる圧力調整は，P1D*≧P1(安全)を維持する P1 の調整が誤って許容限界（最大許容圧力）P1D*を超えるのを防ぐため，安全弁等を用いて外部への空気の放出によって実行される．動力調整部で用いるレギュレータは，過圧に対するリリーフ機能を兼ねると見なされ，一般に安全弁等の必要を生じないと思われがちであるが，リリーフ機能には弁の固着による危険側故障が含まれるため，リリーフ機能によるレギュレータの圧力の調整は，安全(確認)の原理が適用されるべきと考えていい.

圧力 P1 をセンサによって常時監視し，P1D*<P1（危険）のときは動力源を遮断するインタロックを構成すれば, P1 の監視で検知される危険側故障はすべて安全側(停止側)になるよう改善されると思われる．

６－６　圧力監視の構成

P1 には，初期の設定作業が存在する．それは運転圧力として例えばレギュレータの調整などは人によるが，人の設定にはミスが生じやすい．初期設定で P1D* <P1 とする誤りで生ずるリスク発生の原因は解消されなければならない. P1D*より低い圧力 P1 を初期設定する場合，人による設定の危険側誤りを排除するために用いるセンサの構造が提案される（7－8－3 項）．しかしたとえ P1 の正しい設定がなされたとしても，それを維持するレギュレータには，圧力上昇側弁の“開側固着”，及び圧力下降側弁の“閉側固着”という危険側故障が生じ得る．さらに，P1D*≧P1(安全)であっても，異常に小さな P1 が生じた場合も必ずしも安全とは限らない．例えば部品の接合部が外れて空気が噴出しているために圧力が低下しているといった状況である．このような場合，緊急の動力源遮断を必要とするが，現状のレギュレータでは対応できていない．したがって，P1D*≧P1≧P1Lw として，下限の判断基準 P1Lw を設定するのが好ましい．ここに P1Lw は低圧側の異常の判断基準を示すしきい値である．ただし，設計時に固定して使用する場合は P1Lw*と表現する．

ところで，低圧側のしきい値 P1Lw*が有効なのは，現実のインタロックシステムには動力源遮断が含まれ，P1<P1Lw*(異常)を検知したとき動力を遮断して空気の噴出を止めることができるためである．異常な圧力低下が高圧の空気の噴出を示すとすれば，人間が危険状態に暴露される時間をできるだけ短くするためにも，異常を検出後，速やかに動力源遮断すべき要求があって当然である．２つのしきい値を持つこと（すなわち“窓特性”（蓬原，向殿，1989)）によって，安全側と危険側のどちらの故障も検知され，動力源が遮断された状態で人による安全な修理を行うことができる．安全側故障の対応についてはこれ以上の議論を控えるが，纏めると，次の式(6-3)で示すように，P1 が P1D*≧P1≧P1Lw*を満たすとき，改めて **Q1**=1 とし，安全かつ正常な調整が順調に実行されていると見なしていい．

$$\begin{aligned} \mathbf{Q1} &= 1 \quad ; \quad P1D^* \geqq P1 \geqq P1Lw^* \\ &= 0 \quad ; \quad P1 > P1D^* \quad \text{または} \quad P1 < P1Lw^* \end{aligned} \tag{6-3}$$

図 6-3 は，安全の条件 **Q1** を確認して判断結果を **Qg1** として出力する“窓監視”の特性を持つセンサを示す．これはブルドン管のパイプの先端にスリットを備えている．フォトインタラプタでスリットを通過する光を検知しているときは「安全」の判断を出力 **Qg1** として生じ，光が検知していないとき「危険」として出力 **Qg1** を停止する．**Qg1** はセンサによる安全の判断結果を示す 2 値の論理変数であり，安全を 1，安全でない(危険)を 0 とし実用

的には論理的出力としてリレー出力(ON／OFF 信号)で表わされる. **Qg1** は式(6-3)を検知範囲（窓）とする次式の安全の判断を示す.

Qg1　= 1　;　Sg(P1D*) ≧ Sg(P1) ≧ Sg(P1Lw*)　(6-4)

= 0　;　Sg(P1) > Sg(P1D*)　または　Sg(P1) < Sg(P1Lw*)

ここに，Sg(P1D*), Sg(P1), Sg(P1Lw*)は，それぞれ P1D*, P1, P1Lw*に対応するセンサ出力である．センサの“窓特性”（フェールセーフ特性）については後述することにし，ここではスリット構造に注目すると, 式(6-3)の安全の条件 **Q1** がそのままスリットの窓に固定されており，上限のしきい値 P1D*（前報（中村他，2013）における P1max）と下限のしきい値 P1Lw*の間で光が検知されれば，レギュレータ M による圧力 P1 の調整が正常（安全）に実行されていると判断される．ここに **Q1** は，あくまでも安全に対する論理的条件であることに注意を要す.

論理的要求としての安全 **Q1** が現に実行されていることを図 6-3 のセンサを用いて確認する場合, センサには P1D*<P1(危険)を検出できないとする危険側故障が生じうる. すなわち, スリットを通過する光が「ない」という時，誤って「ある」と判断する側の危険側故障は許されないと言うことである．このセンサによる安全 **Qg1** は，スリットによる安全の条件 **Q1** に対する確認を示すが，安全（**Q1**=1）のとき“安全でない（**Qg1**=0）の誤りは許されるが，少なくともに **Q1**=0 であるとき“安全である（**Qg1**=1）”の誤りは生じないとする関係，すなわち次のような論理的ユネイトな関係が成立する.

Q1 ≧ **Qg1**　(6-5)

このようにユネイトな論理的関係（詳しくは文献（川西，1971，蓬原，2007）参照）を達成するセンサを実現すれば，誤りを含む Qg1=1 で生じうるリスクの発生の問題を解消できる．そのため，前報（中村他，2013）にも示した通り，安全の確認に窓特性を持つフェールセーフ論理演算回路（ウィンドゥ・コンパレータ）を用いて解決しようとするものである.

６－７　動力源遮断の構造

図 6-1 における P1*は動力遮断装置における設計上の要求を示唆する．一般に，レギュレータ等，圧力（P1）を供給する設備は，安全の条件で圧力（P1）を調整・保持する機能を有することはいうまでもないが，危険が生じたとき元圧（圧力源）から調整系を切り離すための遮断機能が必要である．また場合によっては遮断に伴って，圧力（P1）を外気に放出して本質的安全状態（P1=0）を生成する機能が求められる．ここでは，図 6-2 の駆動調

整部の入り口に配置される動力遮断装置 V*として遮断条件を備える構造の最も簡単なシャットオフ電磁弁を用いた場合の故障特性について論理的検討を加える．すでに図 6-1 では，遮断弁の特性を **P1*** （=**P1**･**P***）で表わした．ここに **P1*** は遮断弁の状態を示し，正常のとき“非遮断”を，**P*** は“フェールセーフ”，すなわち遮断弁がフェールセーフであることを示し，また **P1** は改めて“圧力 P1 の状態”，すなわち圧力 P1 の調整が正常であることを示し，それぞれ 2 値の論理変数で表す．

ところで **P*** （フェールセーフ）は，故障時における弁の遮断特性を示す．現実の遮断弁の非遮断 **P1*** は，このフェールセーフの性質と圧力調整の正常性 **P1** が組み合わされて（論理積）実現される．ノーマルクローズ型（通常時閉型：NC）の遮断弁は，非通電時における「閉」状態（すなわち遮断）が確保されるので電気的故障に対してフェールセーフ（**P***=1）である．そのため，電気的故障(**Qg1**=0)による遮断(**P1***=0)が保障される．非遮断 **P1*** が少なくともフェールセーフを条件とすることから論理的に **Qg1**≧**P1*** の関係がある．これによって **P1**≧**Qg1**(安全且つ正常)で生ずるセンサ出力を増幅して作られる電流で遮断弁の「開」動作を行って非遮断 **P1*** （=**P1**･**P***）を生成すると言える．

一方，“遮断”は，**P1*** の否定（ちなみに論理否定として記号￢を用いる），すなわち￢**P1***=￢**P1**∨￢**P*** で実行される．ここに，￢**P***=0 であり，ノーマルクローズ型弁はフェールセーフであるために遮断は故障による．したがって，危険（**P1**=0）のとき遮断とするためには，危険を故障（**Qg1**=0）と見て **P*** のフェールセーフの特性を利用する．すなわち，危険／故障を非通電（**Qg1**=0）として遮断される特性をフェールセーフによって実行する．このように，シャットオフ電磁弁の非遮断 **P1*** （=**P1**･**P***）は，危険と故障のいずれでも生ずる“遮断”を **P1**（≧**Qg1**）≧**P1*** （＝**P1**･**P***）の論理的関係で実現していると解される．

図 6-2 の遮断弁 V*は，遮断に復帰用バネを用いたノーマルクローズ型遮断弁を採用しており，フェールセーフ(**P***)，すなわち危険なとき生ずる **Qg1**=0 だけでなく，故障による **Qg1**=0 の場合も遮断が実行されるという受動的遮断の構造（OFF 遮断）が構成されているのである．

このように，図 6-1 のインタロックシステムは式(6-6)に示す関係で，圧力 P1 を，レギュレータ M によって元圧 Pg を調整して，制御圧力限界（最大許容圧力）P1D*を超えない条件で，安全が確保された圧力源を駆動系 P0 に供給している．

$$P1 = Qg1 \cdot M \cdot P1^* \cdot \&^* \qquad (6\text{-}6)$$

このようにして出力 **P1** の危険側故障の影響を動力源遮断により解消するインタロックシステムを構成した．しかしながら，これによって改めて，システムの故障によるリスク発生の可能性が生じるのであるが，その可能性を解消するには，危険側故障を監視するセンサがフェールセーフでなければならないことを求めている．

６－８　故障監視における窓監視の適用

６－８－１　センサの故障と安全確認形センサ

安全は，確認して改めて「安全」と認められる．安全(確認)の原理によれば，危害の可能性のある制御出力は，安全確認を許可の条件とし，安全が確認できないとき危険と見なして制御出力の許可を停止する．特に，安全を確認するためのセンサには安全確認形と危険検出形があり，危険検出形の採用には特に注意が必要だとされる．危険検出形センサの場合，故障で危険が検出できないと「安全」と判断し危険な運転を停止出来ない可能性（危険側故障）を生ずるからである．

改めて図 6-3 に示したセンサについて述べる. このセンサはブルドン管のパイプの先端にスリットを備え，フォトインタラプタでスリットを通過する光を検知しているとき安全の判断 **Qg1** を生じる．式(6-3)における安全の範囲(窓)をスリットに固定し，安全／危険を 2 値化している．設計時に制限された最大許容圧力(P1D*)が勝手に変更されることは本来許されないことである．**Q1** の窓をスリットとして物理的に固定して使用時に変更できないようにしたのはそのためである．

一般にセンサ出力に判断基準(しきい値)を設け，それを超えたとき動力源を遮断するというのが安全システムとして広く採用される方法であるが，式(6-5)のユネイトな論理的関係を無視すれば信頼性依存となり，このままではリスク発生は避けられない．すなわち **Q1**＜**Qg1** と判断する危険側の誤りがリスク発生の根源である．危険の発生とセンサの危険側故障が同時に生ずることは発生確率が十分小さいとしてリスク発生を無視する傾向が見られるが，ここでは，リスクを評価して許容の判断を求めるのでなく，リスクの影響を解消する方策について検討する．

６－８－２　窓特性の適用

スリットの上限を P1D*として固定し，光がスリット内を通過していれば，P1D*≧P1 として「安全」と判断し，その判断結果を **Qg1**=1 として生ずる．**Qg1** はセンサによる **Q1**=1 の確認の意味を持つ．圧力 P1 をブルドン管による機械的変位に変換して捉え，安全の判断基準 P1D*は，センサ出力がスリットの上限の位置にくるよう固定される．スリットによる判断の固定は国際規格 ISO12100 におけるポジティブ結合に相当し，少なくとも，安全の判断が故障（初期調整の誤りを含む）で変化するとされる問題はこれによって解消される．

次に，スリットを通過する光の検知であるが，センサには安全確認形の論理を用いて，光を正常に検知したときのみ安全の判断結果 **Qg1**=1 を生ずるよう構成する．しかし，P1D*≧P1(安全)であっても，光量が十分でなかったり，フォトインタラプタが故障しているときは **Qg1**=1 は生成されない. これは, ユネイトな論理的関係 **Q1**≧**Qg1** に基づくもので, **Qg1**=1

となる側の故障を危険側故障とし，これを排除する目的に応える構成である．これを実現すれば，少なくとも，P1D*<P1(危険)に伴うリスク発生の原因は解消されると考えていい．ところで，スリットを通過する光は「安全」を示すが，それを確認するセンサの故障モードには，上昇側と下降側の両方が存在し，このことはフォトインタラプタにも言えることである．この場合，安全 **Q1** を **Qg1**=1 として確認するためには，式(6-7)によってセンサが正常であることを示す必要がある．

センサは一般に検知対象から抽出した小さな電気信号を“有意”と判断できるレベルに電気的増幅がなされる．忠実度（fidelity）の概念があって，式(6-7)のように，情報として有意と言える信号の範囲が規定される．

式(6-7)の SgUp および SgLw は P1 が信号として”有意”と言えるセンサ出力の上限および下限である．この範囲を上／下に超える信号出力は，もともと信号(情報)として有意性が認められない．ここでセンサによる安全の確認式(6-4)は式(6-7)により有意性が示されなければいけない．

$$SgUp \geqq Sg(P1D^*) \geqq Sg(P1) \geqq Sg(P1Lw^*) \geqq SgLw \qquad (6\text{-}7)$$

ところで，式(6-5)によるユネイトな論理的関係 **Q1**≧**Qg1** がここでも成立していなければならない．この場合のユネイトな関係とは，P1 が安全である時(**Q1**=1)センサの判断 **Qg1** が必ず安全を示すとは限らないが，センサによる判断が安全を示す時(**Qg1**=1)は，必ず P1 は安全(**Q1**=1)でなければならないとする関係である．故障時 **Qg1**=0 となる特性をフェールセーフと言うが，その保障があって初めて，式(6-7)による安全の判断 **Qg1**=1 には誤りが含まれないと言えるのである．このようにフェールセーフの条件で **Qg1** を達成すれば，危険側故障（**Qg1**=1）で生ずるリスク発生の可能性を解消できる．ここに，前報（中村他，2013）に示した，安全の確認に窓特性を持つフェールセーフ論理演算回路（ウィンドゥ・コンパレータ）を採用する理由が存在するのである．

６－８－３　ウィンドゥ・コンパレータと窓特性

“窓特性をもつフェールセーフ論理素子を使ったインタロックシステムの一構成法”（蓬原，向殿，1989）及びその他論文によるフェールセーフ・ウィンドゥ・コンパレータ実現手法に本論は依拠するものであるが，図 6-4 はトランジスタ Q，ダイオード D，抵抗 R による発振部 OSC，増幅部 AMP，整流部 REC でフェールセーフに構成される論理演算回路を，図中の式に示す窓特性（抵抗器で設定される 2 つのしきい値）を持つウィンドゥ・コンパレータとして利用したものである．ウィンドゥ・コンパレータは，入力レベルに対して 2 つのしきい値を持ち，センサからの入力電圧 V が定められた範囲（$V_H \geqq V \geqq V_L$）にあるときに限定して交流信号(この場合 **Qg1**)を出力し，それ以外の時は交流信号を出力しない．

電源電圧とは異なる電位へのレベル変換による発振回路の構成，交流回路の利用により直流に比べエネルギーレベルの高い交流信号を発生する構成，故障時はそのような信号出力が生じない回路の構成等，フェールセーフとしての特徴を有する．このように判断結果を直流でなく交流とする理由については文献にゆずる（蓬原, 向殿, 1989, 坂井, 白井, 2000, 日本労働安全衛生コンサルタント会編，2000）が，実際には，交流出力 **Qg1** は整流され，電磁リレーの出力で示されるので，そのリレー出力が論理出力 **Qg1** であると見なすことができる．ただし，ウィンドゥ・コンパレータを構成する抵抗その他の回路要素はいずれも交流信号を停止する側(安全側)の故障となることが報告（蓬原，向殿，1989，日本労働安全衛生コンサルタント会編，2000）されており，また，窓特性（V_H—V_L）については，抵抗で定まるが抵抗器（炭素皮膜抵抗器）の過電力強制劣化試験で約＋10%の変化後に断線に至るので，窓変動としてこれを配慮すれば安全側の故障モードであることが示されている（蓬原，向殿，1989）．

改めて，これまで述べてきたように，図 6-3 に示されるセンサ構成から信号を抽出し伝達するのは窓構成を通して行われる．ここで窓の外側の判断は「危険」だけでなく「不安」すなわち安全（**Q1**=1）でありながら，それが確認できないと言う場合の **Qg1**=0 を含んでいる．スリットを通過する光によって **Q1**=1 を確認する場合，スリット外にある光は明らかに受光されないが，センサが敏感であるために微光に反応したり，故障で光がないのに誤って発振することがあってはならない．ウィンドゥ・コンパレータは，有意な信号を取り出すための窓特性をもち,センサ出力Ｖが窓(V_H－V_L)の外にあるとき発振停止(**Qg1**=0)となり動力源遮断によってリスク回避が実現される．この場合，ウィンドゥ・コンパレータの窓（V_H－V_L）は，式(6-7)の Sg(P1D*)≧Sg(P1)≧Sg(P1Lw*)に対応して上限のしきい値は Sg(P1D*)を考慮して，下限のしきい値は Sg(P1Lw*)を考慮して設定されることは言うまでもない．このように，式(6-3)～(6-5)の関係をフェールセーフに構成することが要請されるが，安全確認は，式(6-8)のように安全を示す 2 つの“窓”が式(6-8)のような相互にユネイトな関係（ただし式(6-8)は大きさの関係で示す）を維持して実行されると言う理解も可能である．

(**Q1** の窓) ≧ (**Qg1** の窓)　　(6-8)

このように，安全の要求がなされた場合，**Q1**=1 を維持する操作をより正確に行うと言うだけでなく，実際に **Q1**=1 であることを確認してその結果を改めて **Qg1**=1 として示す必要があるのである．**Q1**=0（危険）のときはもとより，**Q1**=1 が確認できないとき **Q1**=0 と見なして判断結果を **Qg1**=0 で表し，これは動力源の OFF 遮断（ノーマルクローズ型の特性）に連動される．そしてこれらのことが，曖昧な信号を排除して **Qg1**=1 に誤りを含まない信号処理のためにフェールセーフ・ウィンドゥ・コンパレータの窓特性を採用する理由である．これにより **Qg1**=1 であれば，必ず **Q1**=1 でなければならないとするユネイトな関係

Q1≧Qg1 が実現される.

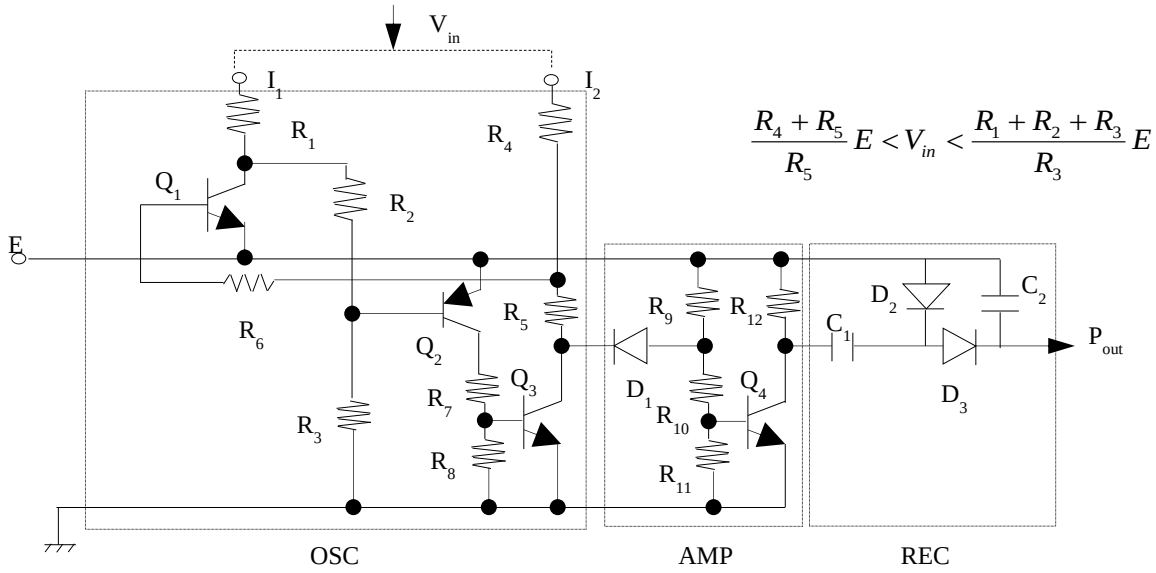


Fig.6-4　Window-comparator (fail-safe AND-gate) (Japan Association of Industrial Safety and Health Consultants ed.,

６－９　インタロックシステムの機能

ISO13849-1 は，安全関連部と非安全関連部を別に扱うよう求めている．著者らの理解によれば，安全関連部とは安全機能の実行を担当するハードウェアであり，図 6-5 のように，安全確認を受ける側を非安全関連部，安全確認を実行する側を安全関連部として，両者の間にはインタロックが構成されている．これまでの検討から，安全関連部としてのインタロックシステムの重要な要件は，設計者によって規定される「安全」をユネイトな論理的関係で実行する安全確認機能（**Q1≧Qg1**）と遮断機能のフェールセーフの要求（**P1***）と言える．改めて，インタロックシステムの有する安全機能についてまとめるとこの通りである．

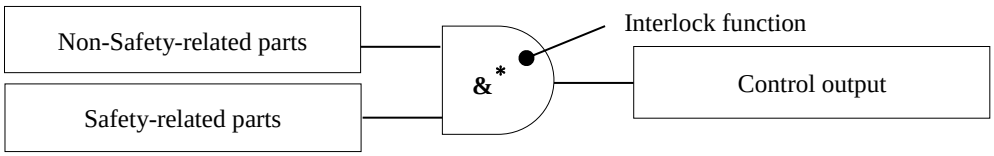


Fig. 6-5　Separation of non-safety-related parts and safety-related parts in safety control system. Separation has been required by ISO13849. The authors have understood to be a request for the interlock. Safety-related parts as the interlock can perform permission / non-permission of the execution of the non-safety-related parts. This interlock has configuration of the function of safe-confirmation and shut-off. This function requires fail-safe.

６－９－１　安全機能の構成

空気圧駆動システムではレギュレータの P1 の初期設定, 異常停止の原因の措置と再起動, 修理・保全など，人手作業が存在する．特に，**Qg1**=0 による OFF 遮断後の再起動は，異常

の原因を排除した後，人の操作によって **Q1**=0 から **Q1**=1 の“窓”による通常の運転状態に復帰する必要がある．この操作を可能とするために強制的に **Qg1**=1 を作り出すためのホールド・ツ・ラン構造のスイッチ等の手段が準備される．非定常の人手作業は別途検討を要するが，あくまでも，人間は，安全機能を担うのでなく安全機能の条件を管理する立場である．再起動における圧力 P1 の再設定は，その範囲が，設計で規定された安全範囲としてセンサスリットによる窓（**Q1**=1）で固定しているため，人間の設定における危険側誤りの可能性は解消されている．

一般的機械の要求では窓の中（安全条件）にあるとき機械の実行が許可され，安全条件にないとき機械の実行は禁止される．本システムでは，フェールセーフなウィンドゥ・コンパレータの窓監視によって，レギュレータ等空気圧コンポーネントの危険側故障の影響が解消されている．

６－９－２　窓監視機能

“窓監視”はシステムの運転中における圧力の挙動を監視する機能であり，動力調整部 P1 の圧力の上限と下限にしきい値を設けて両方のしきい値の内側にあることを運転許可の条件とする．センサによる監視が，常時なされており，また，ウィンドゥ・コンパレータは 50KHz の交流処理を行ってセンサの故障をチェックしている．センサによる安全確認は常時実行されていると見ていい．

６－９－３　停止機能

“窓監視”によって圧力が窓の外側（**Q0**=0）を示した場合，**Qg1**=0 となって P1 は遮断される．また，センサの故障，ウィンドゥ・コンパレータの故障など **Qg1**=0 となり **Q0**=0（安全未確認→危険）と見なして **Qg1**=0 が運転に介入して遮断弁により動力遮断（**Q0**=0→**P1***=0）が実行される．さらに，遮断操作は受動的に行われるため，遮断弁自体が，例えば供給する電流が断線しても，遮断弁の遮断が実行される．フェールセーフとは OFF 能力による安全機能である．安全が確認できないとき，確実に出力を OFF する受動的動力遮断の能力を伴う．インタロックシステムの故障は本質的安全状態を保証する．これはインタロックシステムの故障でリスクが増大するのでなく，故障によるリスクを生じさせない構造である．

６－９－４　調整機能

もともと，誤りのない圧力の設定と，リリーフ機能（安全弁としての機能）をもつレギュレータが完全であれば，安全のために遮断機能を持つ必要はないと言える．空気圧，特

に高圧の空気圧は大きな被害の潜在性を有する危険源であり，安全の厳格な要求に対して，危険側故障やミスを存在させるレギュレータや人間が応えるのはもともと不可能である．本研究では，安全関連部と非安全関連部をインタロックで分離することによって，危険の発生は「停止」に置き換えられるため，人間による調整を含めて，レギュレータ等調整系は，非安全関連部として危険側故障とは無関係に，圧力調整の本来的機能の性能／信頼性等（パフォーマンス）の向上に専念できる．

６－１０　国際規格による評価

６－１０－１　関連する国際規格

インタロックシステムに関係する国際規格は主に次の 3 つが該当し，これによりインタロックの構成法および機能について関連性と相違点について検討する．

（ｉ）ISO12100-1（機械類の安全性－設計のための基本概念，一般原則－第 1 部：基本用語，方法論）

（ⅱ）ISO12100-2（機械類の安全性－設計のための基本概念，一般原則－第 2 部：技術原則）

（ⅲ）ISO13849-1（機械類の安全性－制御システムの安全関連部－設計のための一般原則）

６－１０－２　ISO12100-1，2 による評価

安全機能とは，危険を予測して事故を防ぐ機能，あるいはそれに関連してリスクを下げる機能と言うことができる．ISO12100-2（2003）によれば，「故障がリスクの増加に直ちにつながるような機械の機能」すなわちリスク低減機能（故障でリスクが増大する機能）だとされ，さらに安全関連部は，安全機能を実行するハードウェアと考えていい．インタロックシステムは，明らかに安全機能を実行する安全関連部と認められる．しかし，インタロックシステムにおける安全の立場は，リスク低減機能をそのまま安全機能とはしていない．本論において「事故を防ぐ」とは，事故が生ずる前に危険な行為を停止することだと定める．安全機能は，単に止まるというのでなく，事故の前に止まる“保障”を求める．

ISO12100 は，安全の対象を主に人間が被る危害に置く．したがって，対象とする機械やシステムに人間がどう関わるかによってリスク評価が大きく変わる．空気圧駆動システムは医療機器などの人間と密接な関係で使用される場合から自動化ラインなど人間と離れて使用される場合まで用途が幅広い．そのため，アクチュエータに関して様々な形を取ることになるが，ここでは空気圧供給システムとして，インタロックシステムは，使用とは関係なく動力遮断によって無条件に安全確保するとする立場に立ち，ISO12100-1 の 5.2 項「機械の制限に関する仕様」の“使用上の制限”，“空間上の制限”に関して安全上の特別の条

件を要求しない．したがって，アクチュエータの人間に関わる安全は，空気圧供給システムの安全要求の上にさらに検討する必要がある．

ISO12100-2 の 4.11「制御システムへの本質的安全設計方策の適用」は，制御システムの設計方策として安全関連性能が十分リスク低減できるように慎重な選択を規定する．そこでは正しい設計により，予測できず，かつ潜在的に危険な機械の挙動を回避することが求められるが，窓監視は危険な故障事象を検知して動力源遮断を行い，危害防止の要求に応える構成をとる．また，機械の集合体は，非常停止，保護装置による停止，及び／又は遮断およびエネルギーの消散に対して，いくつかの区分に分ける場合その関係を明らかにしなければならないが，本インタロックシステムは，人間の調整操作，機器による調整機能，安全の確認，危険時の遮断という一連の安全の基本に関わる構成であるばかりでなく，安全機能自体（安全関連系）に故障が生じたとき遮断によってリスク発生を阻止しており，制御システムの本質的安全方策の要求に応えるものと言える．またこれは ISO12100-1 の 3.19 及び ISO12100-2 の 4「本質的安全設計方策」で優先すべき危険源除去の要求に応える方策であると評価されてしかるべきである．

インタロックシステムは安全であることを確認して許可／禁止を行っているが，これは 4.11.3「機構の起動／停止」にあたり，またこの項では 2 値論理の要素（1 の状態を最も高いエネルギー状態で表し，起動は 0→1，停止は 1→0）を考慮することが示されるが，本論の 2 値論理は，安全かつ正常でエネルギー出力において仕事の実行“1”を行い，それ以外及び故障におけるフェールセーフとして停止“0”が達成される．

具体的にも，圧力の上限と下限のしきい値による窓監視は連続監視であるが 4.11.6 「自動監視の使用」の要求に適合している．またここでは触れなかったが，遮断弁による動力遮断と同時に行われるべき排気は 4.11.5 「動力供給の中断」と 5.5.4 「遮断及びエネルギーの消散に関する方策」で要求されるが，これはシャットオフ電磁弁の代わりに排気が付いた 3 ポート弁を用いることで残圧（危険源）の除去に対する要求に対処できる．

図 6-3 の窓監視用のセンサ，ウィンドゥ・コンパレータなど，基本的には 4.12.2「“非対称故障モード”構成品の使用」に適合しており，特に遮断弁はノーマルクローズ型を使用して，故障確率の最小化でなく安全側故障としてフェールセーフを強く意識した非対称故障モードの構成を採用している．

これらの考察により，インタロックシステムは，ISO12100-1，2 の要求に応えるものと評価できる．特に，空気圧駆動システムの圧力調整系の危険側故障の影響(危害)を動力源遮断により防ぐとする目的を実現するものとなっており，このことで，リスク低減の考え方から，リスクの発生そのものを予防するとする本質安全設計方策を実現する実用的なシステムであると評価されてしかるべきである．

６－１０－３　ISO13849-1 による評価

ISO13849-1 はタイプ B 規格であるため，その指針はタイプ A 規格である ISO12100-1,2 により示されるが，機械における安全性の目標を達成すべく，安全機能としての制御システムを実現するために適切な設計を行うための規定である．ISO13849-1 は制御システムの安全関連部における，設計のための一般原則を示しており，安全関連部とは 3.1.1 に「安全関連入力信号に応答し，安全関連出力信号を生成する制御の部分」と定義されている．安全機能はリスク低減機能として示されるが，安全関連部の設計によりその性能が規定される．そしてインタロックシステムは ISO13849-1 の 5「安全機能」として評価する対象である．

インタロックシステムによって行われる窓監視，動力遮断による停止，動力遮断と同時に行われる排気は，5「安全機能」の安全関連停止機能，診断等における監視，非常停止機能，隔離及びエネルギーの放散機能に該当する．窓監視のセンサから出力される電圧とウィンドゥ・コンパレータから出力される交流信号がそれぞれ，4.4 の「安全関連部の設計」に規定されている安全関連入力信号，安全関連出力信号に該当する．また，9・1 に述べたセンサスリットの固定に関しては 4.8「設計の人間工学的側面」に該当し，オペレータの誤使用等で安全関連入力の異常を生じないためである．

ISO13849-1 では安全関連部と非安全関連部は分離して，非安全関連部の制御出力は安全関連部の許可がなければ出力できないインタロックで構成することになる．このことは規格には明確には規定されていないが，インタロック構成上の基本であって，インタロックシステムでは窓監視により「安全」と判断したときのみ動力供給が実行可能となり，窓外にあって「危険／故障」と判断されたときは空気圧駆動システムの動力源は遮断される．また，窓監視の故障は **Qg1**=0 によって遮断弁の OFF 遮断につながり，すべて故障は遮断弁の OFF 遮断の結果をもたらす．その理由で，「異常」は安全／非安全関連部で相互に独立していると見ることができる．このように，インタロックシステムは遮断の構造までを含むシステムとして，残留リスクを容易には認めないとする厳格さの点で，危険側故障率で評価する規格とは異なるが，これは規格においてフェールセーフは危険側故障がない理想的位置付けであり，フェールセーフに為しえないという評価を危険側故障率として行っている表裏関係であると解釈できる．ゆえに基本的には，ISO13849-1 の要求に適合する安全関連システムであると見なすことができる．

そして，安全関連部そのものの評価としては，ISO13849-1 の 6「カテゴリ及び各チャンネルの MTTFd（危険側故障までの平均時間），DCavg（平均自己診断率）及び CCF（共通原因故障）との関係」では特定の PL（パフォーマンスレベル）を達成するための基本的なパラメータであるカテゴリで評価することを要求している．ここにカテゴリは“B，1～4”までの 5 段階の評価を危険側故障発生確率の低さで評価していると言える．インタロックシステムを構成する遮断弁，センサ，ウィンドゥ・コンパレータは故障が発生しても危険側故障にならない非対称故障モードを要求するばかりでなく，繰り返すように，危険側故障が安全側(停止)となってリスク発生を阻止することを保障する．これは FMEA で示した

ように，障害の影響が圧力変化として現われ，その回避，検出のための圧力監視構造が停止装置に直結しているがゆえである．そのため，カテゴリ評価では最高のカテゴリ 4 を超える評価が期待できる. このように, インタロックシステムはシステムとして ISO12100-1,2 および ISO13849-1 の要求に適合するばかりでなく, 本質的安全設計方策としてカテゴリの制約を受けない汎用的な安全関連部（系）を実現していると評価できる．

６－１１　停止コンセプト

国際規格では，安全関連部における「安全」が何によっているのかが明確にされていない．したがって，安全が確認できないとき事故の前で停止すべきとする厳格な停止の条件が規定されていない．曖昧を含む本質から，「安全」は確率的事象（リスクベース）とせざるを得ず，そのため致命的と言えるような大きな被害を伴う事故への適用には明らかに限界がある．これに対して，インタロックシステムは，安全を確認して危険の可能性のある機械的制御を“許可”する機能（安全機能）を実行するハードウェア（安全関連部）である．インタロックシステムによる安全確保は決定論（確定論）に基づく．それは安全の条件の中で“停止”を要求しているからである．したがって致命的と言える被害をもたらすような事故の対策にも適用可能と思われる．このように，2 つの見方から安全の妥当性が論じられている現状において，これらの整合化が可能か否かを検討することが本論の趣旨であった．

本研究で提案されるシステムは，安全（確認）の原理に準拠し，危害の可能性を有する機械的出力が「安全」を許可条件とする構成であり，安全が確認できないとき（危険／故障）の機械的出力の禁止（停止）とともに動力源を遮断する．リスク発生の要因である危険側故障の影響を動力源遮断で防いでいる．本システムは，単に危険側故障の発生確率を小さくするという考え方でなく，図 6-1 で最初に示したように，インタロックシステムを構成し，危険側故障で生ずる危害の可能性を消滅するとする安全のコンセプトを実現する試みである．

国際規格においては，例えば式(6-3)において P1D* <P1（危険）のとき **Q1**=1 となる誤りをリスク（確率）の問題として受け入れようとする．つまり停止できない機械の運転が，リスクが小さいとして許容される場面が想定される．インタロックとは P1D* <P1（危険）によるリスク発生自体を予防するものであり，何よりも，P1D* <P1（危険）に対する動力遮断(停止)を前提とする構成である．国際規格においては絶対安全はないという前提でのリスク評価であるが，停止不可能な機械，あるいは停止の制御が曖昧な機械は，停止の構造を確保して，できる限りリスク（確率）に依存しない安全を確保すべきと思われる．

改めて結論を述べれば，本研究は，安全確保のシステムに対する基本として，故障を単に安全側とするのでなく，危険側故障の可能性に対して動力源遮断による負荷の停止を実行すべきとする主張に基づくもので，これを実現したインタロックシステムは，危険側故

障の影響（危害）を与えない理想的な安全関連系と認められてしかるべきと考える．

６－１２　小括

安全は，確認して改めて「安全」と認められる．本研究では安全のコンセプトを安全(確認)の原理に置き，故障で安全が確認できないときを「危険」と見なして“危険な仕事出力を停止する”とする安全のコンセプトを実現するためのインタロックシステムを提案し，特に本報告では，リスクベースとする国際規格による安全関連部との関連性についての論理的検討を行った．その結果，国際規格による安全の要求は安全（確認）の原理に矛盾するものでなく，インタロックシステムは国際規格 ISO12100-1，2，ISO13849-1 に適合する実用的な安全関連部（系）であると判断される．

空気圧駆動システムにおける安全のコンセプトを改めて述べれば，システムを構成するコンポーネント（13 種類）の故障による危害だけでなく，そのために講ずるインタロックシステム自身の故障による危害の防止を達成することだと言える．空気圧コンポーネントに危険側故障の存在が認められ，その対策として導入したインタロックシステムにも危険側故障の存在が明らかにされ，故障を安全側とする技術（フェールセーフ）が要求される．インタロックシステムは誤りのない安全確認が徹底的に追求され，論理的に安全と言える条件 **Q1** が設計者によって提示され，これとユネイトな論理的関係で確認された安全 **Qg1** に準じて安全制御が実行される．そのために導入した“窓監視”に使用されるセンサ，ウィンドゥ・コンパレータは，故障が安全側となる非対称故障特性を有するばかりでなく，たとえ危険側故障が生じても遮断されて安全側停止となる．リスク低減とする代わりに危険時の緊急停止によってリスク発生を防ぐとする点で，リスクベースの国際規格とは異なるが，緊急時の停止が実質的にリスク低減をもたらすと考えれば，安全（確認）の原理が志向する安全とリスクベースの安全とは本質的には同じとみて矛盾はない．このことを本章の結論としたい．

第 7 章　総括

7－1　システムにおける停止構造の考察

安全は“安全の原理（杉本，蓬原，1990)”により示されるが，「安全確認における運転許可，安全が確認できないときには禁止（停止)」と言える．“安全”が関係してくる作業とは，危険なものを“安全に”扱う作業であり，機械と人間の協働（共存）作業の実現が機械安全では求められていると考察した．そこで機械に求められるのは自律性であり，その自律性とは安全確認という形式に在る．安全が確認された中に自由があり，そこを逸脱しないという自律性が求められる．「安全を確認する行為」において“やめる”ことこそが主体性確保の根拠であり，それは停止による安全の確約である．事故の前で止まることを確約するためにこそ確認という形式が必要になる．本論で示す自律概念・制御概念とは運転（共存）において関係性（危険源との関係で仕事をする）を持つことであり，それは安全の制約（危険源と離れている）の中で許可される．それゆえ制約の中に維持することが，目的よりも優先する．そして制約という明確な制限に対してそれを確実に超えないことを確約する停止でもって判断（確認）基準が示される．安全が確認できないときは自らでもって自らを禁止（停止）することであり，あらゆる関係性（可能性）を断つことであり，それゆえ事故との関係性（事故の可能性）を断つことである．

それは真の意味での独立を確保することである．独立とは強さといった表現がなされ，あらゆるものを従属させているかのような「支配的強さ」に受け取られる．しかしそれはあらゆるものに従属（depend）しない（independent）ことである．独立とはあらゆる関係を断ち (isolation) ながらも“在る”ことにおける強さであり，孤独に耐える強さである．それ故に世間一般的な価値観での華やかで幸せなものではない．事故とはこの関係性を断て（break）なかった結果であり，真に独立を確保しえなかった結果である．停止（孤立：isolation）を持ちえないことが事故の原因である．社会における個人としての独立は，加害者にならないというところにその限度がある．加害者になるとは社会に強制従属（制裁）させられることである．単に停止すればいいのではなく，たとえ自らに被害が出ようとも，この加害者となる前に強制停止するということが，自律を確保するという個人としての尊厳のためには重要である．

各章において強調するのは“やめる”構造であり，それ故に“やめない”ための工夫，積極性といった形で生産・運転システムが形成される．

2 章において，国際安全規格について検討を行った．そこにおいて，機械は“止まる”という停止概念を枠組みとして共有したと考えられる．リスクアセスメントを行うということは，トラブルの選択と言える．取り返しのつかないようなトラブルを，取り返しがつくトラブルへ変えるための選択を行っていると言える．扱いうるトラブルであるから残留を

許容し，そのトラブルに予定（損失補償）通り対処する．このときの主に使われるのが，ガードや停止処理である．傷害事故を「作業において扱いにくいが，トラブルは生産停止」というように変更する選択である．

そこにおいて，生産システムにおいても“止まる”ことを前提に生産システムを構築するということで停止を共有したと考えられる．停止という枠組みの中では，停止に伴う被害とは資産に及ぼす被害であり，人命の被害ではない．それ故に被害を前提とし，計算も可能である．そして停止という枠組みが正常であるからこそ，停止を回避するという稼働率向上が正当に行える．

たとえば，日本では在庫レスによる最高の生産性を達成しようとする．しかし在庫とは生産停止に対するバッファである．バッファがないとき，逆に生産停止の影響が際限なく伝達することになる．その社会的影響に責任を持つとは，止める構造を前提に被害最少を考慮することである．停止安全がない状態においての「バッファがない」とは，作業者に自らの被害に優先して（事故となるまで）「止めないこと」を強要する脅迫である．そしてそれは設計者には，危険側故障を減らすことよりも故障を減らすことの要求になる．例えば，リレーは危険側故障（接点溶着）：安全側故障（接点不良）＝1：10^3 と言われるが，危険側故障を減らすために直列（すべて接点溶着したとき危険側であるなら，2 個なら危険側：安全側=1：$10^3 \times 10^3$）にすることは生産に関する信頼度が減ることでもあり，またそれは安全側ではあるが停まる頻度は上昇する．正当な手続きがなく（止まったときの対処準備はなく），止まることを拒否される（認めない）とは，危険側故障を減らすためであっても故障の増加は認めないということである．これは故障しない機械という「(事故がないから）安全だ」としか言いようがない状態の要求になる．故障しない機械を前提にすると，保守・保全の役割は不明確になる．故障が安全側であれば，事後でも対応できたが，故障しない機械において故障は最後に残る危険側のみとも表現できる．それは事故によってのみ終わることが予定されているともいえる．国際安全規格は危険側故障を減らすことと受け取られるが，安全側故障を積極的に認めていくことであり，安全側としての止まることを認めていくことである．この点に配慮がいかないと，故障を減らすことと危険側故障を減らすことは程度の違いとなり，結局，信頼性が高いものを作ればいいという理解から脱却できない．

3 章において，安全確認で実行されるが，それは不安を解消していくそのプロセスで安心を得て仕事は実行されると述べた．不安を残しながらの仕事はできない．不安を解消する処置がそれぞれの段階できちんと引き継がれて，そこに確証を得ているからこそ，“安心”して仕事ができる．不安を解消するとは，事故の前に止まれることの確証を得ることであり，いつでも止まれる（やめれる）からこそ，自らのコントロールを逸脱する（扱いきれない）という不安から解消される．それゆえ「止められない機械」，「やめられない仕事」というのは独立（自律）がない弱さの象徴であり，不安の根源である．

プラス（生産としての関係性）だけ見ると，繋がりあうことは幸せかもしれない，そし

て“やめる（止まる）”とは否定的な行動であり不要とされる．しかし関係性がマイナス（事故，損害としての関係性）に転化するとき，“やめる”ことができないとは，抵抗しながらも流されるしかない状況である．危険に直面しても，（事故となるまで）回避をし続けることになり，気を抜くことは許されない．しかし切れない繋がりとは，異常時のみ問題となるのではなく，日常においても，そのひずみが弱いポイント（弱者）に集まることで全体（強者）は一時の安定を得ているものである．メンテナンスなど非定常作業と言われるが，本来であるならば非定常作業は定常作業へ組み入れて行かなければいけないものを，あえて非定常とする傾向がある．それは本来非定常であるからこそ代替的な安全対策を組み直していかなければいけないが，その代替策を人の注意でいいとする安易さのためと思われる．例えば，特に危険な作業において，労務管理及び諸費用等を逃れる為の一人親方問題があるが，あえて安全管理システムの中に入れないことを選んでいる．立法精神に沿わなくとも違法と認定されない限り搾取することに何ら違和感を抱かず，むしろ搾取しないことが経済的に非合理となる．J.ベンサムが「最大多数の最大幸福」を唱えたとき，そこにはJ.S.ミルが指摘するように平等の追及がある．一人ひとりが対等であるからこそ，最大多数（個人集計）に対して各人が（消極的にも）了解できる．確率は大数の法則が基本であるが，人間が確率で扱われるとき，そこに一人ひとりの平等はあるのだろうか．リスクというとき，リスクを偏在させ，真にリスクにさらされているのは弱者だけであり，弱者ゆえにリスクを受け入れざるを得ない状況にある．リスクアセスメントで許容リスクというとき，行政も経営者も設計者も安全管理者もリスクにさらされていないが，真にさらされる労働者は，ただ提示されたリスクを受け入れざるを得ない状況である．社会的にリスクで扱うその基礎には，一人ひとりの平等の構築があり，安全はその達成のためである．そして労働者が自らの安全を確認できないときに停止する構造を持てない場合，そこに対等性はない．停止の構造の上に，経営者は労働者の安全確認を如何に創出していくかで仕事の成果を考えなければならない．経営者と労働者は自由な契約を結ぶが，それは対等であるからこそ結べる契約である．

4,5 章において，安全は自律概念で提示され，自律概念とは自らを規定（限界）するものを知ることであり，それを逸脱しないことである．そして真に自律的であるとは“やめる”ことを自らの権利として認識し実行し得ること（構築されていること）であるというのが本論の述べるところである．

それは機械においても同じである．人間の代わりにとなるとき，真に人間の代わりとなるべき自律性を所有していなければならない．それが機械における自己インターロック構造である．オートメーションとは単なる“自動”機械化ではなく，安全を確保する機械であり，それゆえ“自律”機械である．自己インターロックを持つ機械であり，自己インターロックは停止の構造によって規定される．

そしてまた工場における機械の真の使用者は経営者と認識すべきである．経営者は労働者に機械との協働を依頼しているのであり，それゆえ機械の自律性の欠如は経営者におけ

る自律性の欠如である．現実問題として今は自律的な機械が作れないかもしれない，しかし，その代替として労働者に常に押せる非常停止ボタン（労働者に安全を確信してもらうことで ON になりそれ以外では OFF となる）を渡していることで労働者の権利に対して対等となる準備をしたといえる．

また，5 章において特に述べるのは，事故を防ぐとは「事故の前に止まる構造」であり，危険を想定し，危険の前で想定通り止まることの確定性である．そして“事故の前に停止する”という確定性，それを確認するということが「“安全に”仕事をする」という確認構造になる．“安全に”とは隔離状態（危険源と離れている）を作り出しているとも表現でき，制御性（危険を認識し，操作し，離れていると確認する）により隔離は生じているといえる．そして，その無制御性において隔離状態を逸脱しないで停止する（事故の前に止まる）ことにより安全が確約されるものであり，むしろ無制御時における停止を確約することへの妥当性により制御が許可される．また，停止に受動要素が求められるのは，それは恣意性が入らないということで非制御性ということであるが，確定的な特性で示されるということは未来が予言可能ということであり，“やめる”という非恣意的（非能動的）行為において「事故の前に止まる」という未来を確かな確度で確信することである．

停止とは，自身（機械）においては無・可能状態と表現できる．可能性を持つこと自体が無いということである．そしてそれ故に相手への危害が不可能であるということである．機械の停止は人間への危害の不可能性という意味で，完全な共存である．様々な選択肢（可能性）を持つことは，事故（危害を与えること）を回避はできてもその失敗で事故となる．危害が不可能ということは，相手との明確な関係の中で示される必要がある．それ故に事故となる前に止まるということをが，相手との関係の中で示される．

本質安全というとき，接触（危険事象）は可能であっても危害は不可能ということであり，相手（人間）によって止められるということである．リスク（確率）であるとは，契約的に，止めることの遅れ（被害）が（相手に）どこまで許されるかである．リスクは被害を考慮した壊れ方の（構造的）選択としての非対称性である．

停止とは危険（事故）の手前に在るという非対称性の実現である．そしてこの非対称性は加害者とならない非対称性と言える．つまり相手と自身の被害の割合等ではなく，相手という「超えてはならない制限」の前において，自身が持つ可能性自体を無くす構造が停止であり，それ故に自身の存在の可能性を無くす（自身に壊滅的被害を受けても外部に出さない）ことにおいても達成する非対称性でもある．この危害の不可能性とは，結果としての被害の非対称性と言ってもいい．

ヒポクラテスの誓いがプロフェッショナルの倫理として示されることが多いが，その意は「何よりもまず，故意に危害を加えるな」（P.F.ドラッカー，2003）という非対称性の約束であり，それを信じられるがゆえに信頼関係が結ばれる．そして私たちは，自らの行為において，たとえ被害をこうむることになっても加害者にはなりたくないという非対称性を持つからこそ，社会関係を結べるはずである．これは危険な状態において実行はしない，

という非対称性であり，本論では危険の手前で停止することに共通性を見出している．それゆえリスク評価とは停止の失敗による被害（自身 or 相手）が相手のものにならないという非対称性の考慮である．

6 章において，機械における停止とは，機能ではなく本来備えるべき構造であるという前提に立ち，改めて，インタロックシステムと国際安全規格で規定される安全関連部との整合性について検討を行っている．

・安全（確認）の原理は，危険のときだけでなく故障のときも停止して，少なくとも事故を生じえない保証を要求する．そして

・国際安全規格によるリスク低減は，危険源における危害の可能性の如何によって許容リスクを評価する．

国際安全規格は事故防止対象を広く扱っているがゆえに本論は部分的であるかもしれないが，停止安全という概念の上において両論に矛盾はないとする．

一般に機械の持つエネルギーが危害の可能性となる．停止とはエネルギーの消去であり，それは危害の可能性を除去することであるが，あらゆる可能性（目的）を除去することである．停止とは単に危害の可能性のない状態ではなく，可能性（目的）を持ちえない状態である．機械は本来そのような停止を持つことを前提とするのが安全（確認）の原理である．そして，このような停止を回避すべく，離れた状態（運転の継続）を作り出している．事故を回避するとは，事故の前での停止を確保し，その停止を回避することである．

従来，停止とは機能的であり危険回避の一手段でしかなかった．そして回避の連続であり，“やめる”ということは十分には認識されえなかった．またフェールセーフも“壊れたら止まる”というのみである．価値は生産に在り，有産にこそ価値があり無産には価値がないという認識が根本にある．自由と言っても，有産という価値から逃れられない．自由は選択の連続であり，その選択から逃れることができない自由刑（自由であることをやめられない）とも表現されるが，（特に金銭的）価値を生み出さなければ意味がないという強迫から自由になれていない．それは“やめられない”ことの苦しみである．しかし，太古の危険に囲まれた自然状態とは違い，社会を作り技術を構築し経済を発展させとしてきたのはそこに安全状態を作り出すためではなかったのだろうか．人間は生きることをやめることはできない，しかし立ち止まることはできるはずである．社会の安定とは人々にセーフ・コンディションとしての足場を提供することであり，自由のための足場を提供することである．そして人々はその様な社会を構築するためにこそ社会に参加する．

日本では，一度進みだしたらやめられない，また過去の強烈な成功体験が進むことを強要する，ともいわれる．水俣のような公害やサリドマイドのような薬害，またアスベストなど，やめる機会があってもやめることはなく，破綻することで止まるというような状況である．何が起こるか「わからない」とき，「わからない」から「やれる」・「やってみる」とは自律的ではない．自律的とは「わかった」ことを「わかった」ようにやることであり，「わからない」ときはやめることである．そしてこれは「わかる」ことに積極性を持つ人

格としての個人がいる社会でないとうまく回らないであろう．結果ではなく決断に責任を持つからこそ人格が要求される．結果責任は行為が悪くても結果が悪くなければ問われることはなく，結果という外形的なものだけで人格（行為）は関係ない．日本ではよく「規制されたら，やめる（罰せられなければ何をやってもいい)」と言われるが，規制されるということは様々な制約が具体化されることであり，当然全体的であり自社に最適なものではない．そこにおいて，日本では，規制が作られないためにこそ自制した行為が必要であるとはならない．やれることは何でもやって，やりすぎて規制されたらやめる，という状況である．自律的（人格的）であることを他律（強制法規等）で達することはできない．今一度，一旦立ち止まることができる社会，被害を出す前にやめることができる社会を構築する必要がある．

自己インターロック概念は，自律の概念であり，制御の概念である．そして制御において制御可能／制御不可能のどちらかではなく，制御“無可能”とでもいうべき位置を見出すことである．それが“やめる”であり，自らの存在の確保が（破壊につながるような可能性としての）目的を持つことより優先されることである．

「「汝自身と同じように，隣人を愛せ」とか「みずからに為されたくないことを他人に為すな」とか・・・これらはどれも〈自己〉を，すなわち自分とのつきあいを基準としています．(ハンナ・アレント，2007)」とあるように，道徳律は他者とのつきあいを律するのではなく，自己とのつきあいにある．相手との関係性，周囲への迷惑等は本質的な問題ではなく，結果的な評価である．判断の基準を結果(周囲の評価)に置くということは環境従属的であり，環境独立的（主体的）な存在とは別物である．また，たとえ（ナチス時代のドイツの強制収容所のように）合法的な罪であり，「汝，為すべし」と命令されても，「いざ決断を迫られたときに信頼することのできた唯一の人々は，「わたしにはそんなことはできない」と答えた人々なのです．(ハンナ・アレント，2007)」と指摘される．しかし，“為す”ことが重視される世界では「できない」は無能とみられる．そして，“為す”ことがコミュニティに対する責任と追及される．

しかしこの“できない”つまり“やめる”ことができるのが自律には重要である．例えば，車は，通常は事前に減速して正常範囲にあることの確認を継続させ運転を継続する．“やめる”とは，ブレーキを踏むことであり，停止してエンジンを切ることである．ブレーキを踏めない状況とは正常な運転とは言えない．車の運転において停止が完了できる車間距離を常時確認し確保し運転する．確認（確保）できないときはブレーキをかけ停止しなければならない．また疲労した時，たとえやめたとしても，回復したらまた目的地へ向かうことができる．しかしやめることができない場合，（事故で）すべてを失うことになるかもしれない．そしてその影響は社会的（自分のリスクは自分で取れるが，その範囲を逸脱する）である．目的を持つのならその失敗の影響においても考慮すべきであり，失敗しなければ問題ないとなるのは無責任である．そして自身の存在を失ってまで達成すべき目的と

は，自身の能力を超えた目的である．少なくとも日常の仕事において日々持つような目的ではない．やめることができないとは，制御を続けることである．失敗するとは制御不能になることであり，制御不能状態を制御するということは，少なくとも同じコントローラー（単一の人間）ではできない．自己インターロック概念とは，いつでも“やめる”ことができるから実行ができると言え，むしろ不安が停止（やめられること）により解消されているからこそ実行に積極的になれるといえる．これは，受動的安全確保能力があるからこそ，安全を気にせず実行に集中（能動的実行）できるとも言える．

5 章で合目的的制御・安全調整制御・停止制御と 3 つの関連で示したが，これは目的と停止を安全確認構造で分離しているといえる．一般に，多重であるとはそのバランス調整が難しくなる．目的と停止を分けるということは，停止を多重にしても，それは目的の制御性へ影響しないということである．逆に目的において多重にするということは，目的制御同士のバランス調整に資源を割かれ，本来の変化に対する対応能力が削がれることになりかねない．安全確認システムが目的制御と独立に在るとは，目的制御を，安全を考慮せずに（非安全関連系として）自由に設計するためである．そして停止を予定する（空間の確保）とは，そこから離れることは確認における時間的猶予の確保である．この時間的猶予において確認の時間的多重化という可能性がある．空間と違い細分化・多重化が行いやすい．確認機能にわずかでも非対称な誤り傾向がある場合，一回一回の確認の全体に対する影響を小さくし，極端に多く繰り返すことで，その総合（増幅）は非対称性を表してくる．“やめる”構造とは「事故の前で止まる（空間）」構造を「不安（確認できない）で止まる」構造でインターロックを取っていると言える．そして安全調整制御は「不安がない」状態を積極的に作り出し，インターロックの起動を抑制していると言える．これは，安全調整制御は安全確認される中に抑制的に留まることであり，また合目的的制御の逸脱を抑えることでもあり，それは合目的的制御の信頼性を高めることへとつながる．これは止まるシステムに対して，止まらないシステムとして信頼性を高めるということである．

自己インターロック概念は自律概念であり，自律には“やめる”構造が必須なことが本論の結論であり，それは目的に対し“やめられない”ではなく，“やめない”ためにこそ必須である．これは独立（切断，停止，孤立）とは，独立することが目的ではなく，常に独立であることを求めているのではない．相互に自律的な関係を結ぶためにこそ，いつでも独立状態に移行できる条件が必須であるということである．交通信号は赤で確実な安全を作ることを求めるが，常に赤を出していればいいのではなく，青で許可を出すことを目的として確実な赤を求めている．

本論において，安全な状態とは停止である．そして，停止処理（減速等）とリスク低減は同じ方向性を持ち，そこに共通するのは可能性であり，（完全）停止とリスク・ゼロとは可能性が無いという同等性である．このような相似性を持つが，リスクとは運転（実行）許可のためであり，停止能力とは実行における事故回避のためのものである．

「事故の前に停止する」，あらゆる概念はここからの拡張である．どのような概念を持とうとも，基本の条件（事故の前）において基本の概念（停止）に帰着する．目的概念も調整概念も様々な試行がなされ有用な手法が求められるであろうが，それは安全確認システムの許可によるものである．そして安全確認システムは，すべては事故の前における停止という概念に帰着されるという共通性を持つからこそ安全に関する論理といえる．

停止する機械は，危害を与えないという信頼（trust）において，真に人間との共存を可能にしている．そしてその極限として，危険側障害において自らを破壊しても停止の非対称性（事故の前）を確約するクリティカル・インターロックは，「非常の場合に臨んで，たとえ無力であっても，お互いのために，本当に踏みとどまる人びとは，常に限られた範囲の人びとであり，あるいはごく少数の人びとだけであります.」（ヤスパース，1975）と指摘されるように，最も人間らしいが人間には達成が難しい行為の，“自律した機械”による実現である．本論は「事故の前での停止」からシステムを構築することを述べており，事故の前の停止の確定性が，運転システムに生産を追及する自由を与えるものである．

７－２　結論

現状の国際安全規格は，製品のグローバルな流通のための安全認証を目的とし，またリスクベースの安全を指向している．それは背後に補償（保険制度）が控えているためともいえる．それゆえ許容リスクにあることと要求されるが，加害者が被害を補償して済ますことができる範囲は明確ではなく，またそれほど広いわけでもない．そしてその領域に対してコントロールも制限も明確でない．リスク低減処理の追求を行っていても，結果として社会で問題とならない（保険等で事後処理が済む）ことにより安定が保たれていると言える．リスクベースは，影響（リスク）が残ることを前提に，影響を減らすことを求めており，ISO/IEC Guide51（安全側面−規格への導入指針）においても“絶対安全はない”ので改めて評価するようにと指摘している．しかしこれは「安全はない」と表明しているわけではない．あらゆる状況に対して万能な安全ではなく，安全の証明における条件・限界を表明し，安全確保の条件をユーザーまで引継ぐことを求めていると理解すべきである．

一般に安全の評価は危険側・安全側故障の非対称性で評価される．国際安全規格は State of the arts としての安全側（十分に吟味された安全原則など）を求めたうえで，危険側故障の可能性をリスクとして扱うと理念の上では解釈可能であるが，現実として危険側故障が実際に起こる率を求め，その装置を多重にすることで危険側故障率を下げるところに証明性を依拠しているとしか言えない．わかった危険側故障についてはそれを下げることを明示するが，安全側を立証するものではない．特に日本においては，信頼性と割り切ることで，国際規格の適合において，故障率をすべて危険側と置いて減らせばいいとなるが，そこにおいて安全側という概念自体がなくなってしまう．

これまで，事故防止として様々な手段を取ることでリスクが下がるとしてきた．このこ

とは様々な技術を安全技術と認めるが，しかし逆にどの安全技術も不完全と表明するのに等しい．このことは生産性や利便性などと安全性が分離されないままに，経営・管理的側面から適度なバランスとして評価する行為と言えるが，しかしこのことが安全工学をゆがめていると言える．機械安全（国際安全規格）はリスクの形で評価するという点において様々な機械を整合的に扱えるとしてきた．これは端的には人に危害を与えるという点での共通化と言える．リスクの考え方で様々な状況に対応すべく拡大してきたと言える．しかしリスクの考え方に影響され，「事故は防げない」ものであると前提するようになってきたと言える．これは事故防止としながらも，はじめから事故は防げないとして考えるような矛盾に陥っていることになる．「事故を防ぐ」を機械安全（国際規格）成立の原点に立ち返り，「止まる」を安全の基本構造とすることを提示した．

本研究では，事故に関わるとは「事故の前で止まる」ことと限定し，この停止をシステムの非対称特性として扱うことを提案している．安全と関係するのは「止まる」という行為のみと限定する．危険だから止まるのではなく，「止まる」という原則によって，それが事故とかかわるときに危険の概念・安全の概念が生じる．安全に関係するのはこの点のみであり，安全側とは「とまる」ことであり，止まれないが故に事故となる．

追求するとはそこに構造が生じるということである．リスクベースの安全は，その追求によってリスク・ゼロというところに構造（極限値に漸近するか）があるかといえば，必ずしもそうではない．それゆえに，「どこまでやれば安全か？」となるが際限がない（構造がない）追求となる．本論は安全システムに「事故の前に止まる」ことへの妥当性を求めるという帰結であり，機械システムは停止能力を持つこと，それが安全確認型で構成されることとして具体化される．

本論では国際安全規格が安全の原理を妥当性の根拠にしていることを明らかにしている．安全の原理に基づくことで事故の前に止まる完全性を追求することが示される．そして「事故の前に止まる」を妥当性の根拠とした安全の証明に対し，その限界においてリスク（事故の可能性）が生じることを示した．ここにおいて，国際安全規格に対しては「事故の前に止まる」構造を条件とした危険側評価を行うことが要請されることになり，両者の立場は明確になる．

謝辞

最後になりましたが，本研究を行うにあたりお世話になった方々に感謝の気持ちを述べさせていただきます.

直接研究に関するご指導をいただくと共に，幅広い範囲にわたる考えを享受させていただいた，明治大学の杉本旭教授に心より感謝申し上げます.

本研究を学位論文としてまとめるにあたり，副査として有意義なご指摘をいただいた山本俊哉教授，向殿政男名誉教授には心より謝意を表します.

また，本研究は長岡技術科学大学専門職課程（システム安全）から行っており，研究に関して多大なる助言をいただいた福田隆文教授らシステム安全専攻の先生及び修了生の皆様にも深くお礼申し上げます.

また，システム安全研究室の皆さんにはいろいろお世話になりました.

参考文献

安全技術応用研究会編，安全システム構築総覧,初版(2001) , pp.80-81，通産資料調査会.

安全技術応用研究会編，国際化時代の機械システム安全技術，初版（2000），日刊工業新聞社

British Standards Institution, BS EN764-7:2002，Pressure equipment. Safety systems for unfired pressure vessels , (2002)，日本規格協会.

蓬原弘一，非対称誤り素子によるフェイルセイフ論理回路の一構成法,電気学会論文集 C 編, Vol.104, No.2(1984) , pp.29-34.

蓬原弘一，2 値論理を用いて安全原則を考える，日本信頼性学会誌,Vol.29,No.2(2007),pp.80-90.

蓬原弘一,向殿政男，窓特性をもつフェイルセーフ論理素子を使ったインタロックシステムの一構成法,電気学会論文誌 C 編, Vol.109, No.9(1989) , pp.676-683.

蓬原弘一,杉本旭，安全確認形作業システムの論理的考察,日本機械学会論文集 C 編, Vol.56, No.529(1990) , pp. 2378-2385.

蓬原弘一,杉本旭,向殿政男，フェールセーフ・ウィンドゥ・コンパレータの構造とその応用,第 18 回 FTC 研究会資料(1988).

蓬原弘一,杉本旭,向殿政男，安全作業におけるインタロックの構造と実現,電気学会論文誌 D 編, Vol.107D, No.9(1987),pp.1099-1106.

ハンナ・アレント，ジェローム・コーン(編集),中山元(翻訳)， 責任と判断，初版第二刷（2007），筑摩書房，p.93

ISO，ISO12100-1:2003，Safety of machinery-Basic concepts and general principles for design， Part 1：Basic terminology， methodology, (2003) , 日本規格協会.

ISO，ISO12100-2：2003，Safety of machinery-Basic concepts and general principles for design， Part 2：Technical principles, (2003) , 日本規格協会.

ISO，ISO13849-1:2006，Safety of machinery-Safety-related parts of control systems， Part1:General principles for design，(2006) , 日本規格協会.

ISO,ISO/IEC Guide51:1999, Safety aspects － guidelines for their inclusion in standards,(1999),日本規格協会

J-P.サルトル，伊吹武彦訳， 実存主義とは何か，24 版(1959)，人文書院

海保博之，田辺文也， ヒューマン・エラー 誤りからみる人と社会の深層，初版（1996），新曜社，pp. 38～39

日本機械学会編， 安全工学最前線―システム安全の考え方―，初版（2011），共立出版

日本労働安全衛生コンサルタント会編，これからの安全技術-工作機械等の制御機構のフェールセーフ化に関するガイドラインの解説-,第１版(2000) , pp.72-74,中央労働災害防止協会.

日本プラントメンテナンス協会編，入門・機械&保全ブックス 油・空圧の本②,第5 版(2003) , p.179,日本プラントメンテナンス協会.

川西健次， Fail Safe,電気学会誌,Vol.91,No.4(1971),pp.22-28.

Kleinbreuer, W., Kreutzkampf, F., Meffert, K. and Reinert, D., BIA-Report 6/97e, Categorized for safety-related control systems in accordance with EN954-1(1999), Hauptverband der gewerblichen Berufsgenossenschaften (HVBG).

向殿政男，よくわかるリスクアセスメントー事故未然防止の技術ー,初版(2003),中央労働災害防止協会

中村瑞穂,田中慎也,杉本旭，空気圧駆動システムにおける危険側故障を解消するためのインタロックの提案,日本機械学会論文集 C 編, Vol.79, No.805(2013) , pp.167-177.

長岡技術科学大学編， はじめて学ぶ機械の安全設計，初版（2005），日刊工業新聞社

Neudorfer, A.，城結花，ドイツおよびヨーロッパにおける機械安全， 品質, Vol.42,No.3(2012), pp.345-352.

大山博,炭谷茂,武川正吾,平岡公一， 福祉国家への視座 ： 揺らぎから再構築へ,初版（1999），ミネルヴァ書房

P.F.ドラッカー,野田一夫(監訳),村上恒夫(監訳)，マネジメント ―課題・責任・実践（上）,25 刷(2003),ダイヤモンド社,pp.603-604.

坂井正善,白井稔人，フェールセーフ素子について,安全衛生コンサルタント, Vol.20, No.56 (2000) , pp.48-55.

Schuëller, G.I. ,小西一郎訳，構造物の安全性と信頼性,初版(1984) , p.96, p.104,丸善.

杉本旭,蓬原弘一，安全制御系における安全情報のエネルギー伝達，日本機械学会論文集 C 編,Vol.56,No.530(1990),pp. 2658-2665.

杉本旭,蓬原弘一，安全の原理,日本機械学会論文集 C 編,Vol.56,No.530(1990),pp. 2601-2609.

杉本旭,蓬原弘一,向殿政男，安全作業システムの原理とその論理的構造,電気学会論文誌 D 編, Vol.107D, No.9(1987),pp.1092-1098.

杉本旭,粂川壮一,深谷潔,清水尚憲,梅崎重夫,池田博康,芳司俊郎,蓬原弘一，安全確認形安全の基本構造 ： 安全(確認)構造の条件について,日本機械学会論文集 C 編，Vol.54, No.505(1988-9) , pp.2284-2292.

梅崎重夫,杉本旭，中村英夫，産業機械の安全方策に関する基礎的考察ーリスク評価に含まれる不確定性を考慮した安全方策の提案ー，日本信頼性学会

誌,Vol.23,No.7(2001),pp.659-675

ヤスパース，草薙正夫訳，哲学入門，三十三刷(1975)，p.26，新潮社

矢川元基編集委員長，構造工学ハンドブック,初版(2004) , pp.536-537,丸善.

山岸俊男， 信頼の構造 こころと社会の進化ゲーム，初版（1998)，東京大学出版会